Introduced by _____ Council Bill No. _____R 173-12_____

A RESOLUTION

authorizing an agreement with Tele-Works Incorporated for implementation of multi-channel billing, payment and automation solution for utility billing and payment via the internet or telephone.

BE IT RESOLVED BY THE COUNCIL OF THE CITY OF COLUMBIA, MISSOURI, AS FOLLOWS:

SECTION 1. The City Manager is hereby authorized to execute an agreement with Tele-Works Incorporated for implementation of multi-channel billing, payment and automation solution for utility billing and payment via the internet or telephone. The form and content of the agreement shall be substantially as set forth in "Exhibit A" attached hereto and made a part hereof as fully as if set forth herein verbatim.

ADOPTED this _____ day of _____, 2012.

ATTEST:

_____ _____

City Clerk Mayor and Presiding Officer

APPROVED AS TO FORM:

_____

City Counselor

Agreement

for a *Summation360™* Solution from TWI

SUMMATION360™
a TWI innovation

SOW No. 7793d
Project: *Summation360* Solution Suite for the City of Columbia, Missouri

This AGREEMENT (this "Agreement") is made this _ day of _____, 2012 (the "Effective Date"), by and between City of Columbia, a Missouri municipality ("CITY"), and Tele-Works Incorporated ("TWI"), a Virginia corporation with authority to transact business within the State of Missouri. CITY and TWI are each individually referred to herein as a "Party" and collectively as the "Parties".

NOW, THEREFORE, the Parties hereto, for good and sufficient consideration, the receipt of which is hereby acknowledged, intending to be legally bound, do hereby agree as follows:

1. Term. The "Initial Term" of this Agreement shall commence on November 1, 2012 and shall continue for twenty-four (24) months following this date, unless sooner terminated in accordance with the terms herein. CITY may renew the Agreement for up to three (3) additional one (1) year terms ("Renewal Terms") upon thirty (30) days written notice prior to the end of a Term or any Renewal Term.
2. Description of Products and Services to be provided by TWI. TWI shall provide to the CITY the Summation 360 Solution Suite, more fully described herein.

DESCRIPTION OF PRODUCTS AND SERVICES

The *Summation360™* Solution Suite is a hosted, multi-channel billing, payment, and automation solution for utility billing organizations. The specific *Summation360* components to be delivered to the Client under this SOW are described in this Section.

Web / On-Line Services

Summation360 online services include the following components: Pay Now, Portal/My Account, Paperless eBilling, and Mobile. These components are described more fully below.

Web – Pay Now

"Pay Now" is a customer self-service web interface that provides a fast way for customers to pay without having to register an online account. Pay Now includes the following:

- Log-in with account number and the numeric portion of street address
- View account balance and last payment amount
- Pay bills by credit card or eCheck through the Summation 360 system
- Real-time account access and payment posting through the use of the API

Web – Portal / My Account

Through Summation 360, customers, by registering to use the "My Account" portal, will be able to manage payment, notification, and billing preferences, make payments, and log in quickly in the future without having to remember their account number. Customers will also be able to link and pay multiple utility accounts with a single payment. The My Account Portal includes the following:

- Self-register for My Account access; log in with email address and password
- Manage settings to receive a paper or electronic bill
- View invoice history, consumption history, and payment history
- Pay bills by credit card or eCheck
- Set up monthly recurring payments (requires TWI Payment Processing)
- Multi-Account Access:
  - Customers can add multiple utility accounts to their My Account page
  - View payable balances and account status for multiple accounts
  - Make a payment on multiple accounts with a single credit card or eCheck transaction while updating each individual account directly in the host database system
- Real-time account access and payment posting

Web – Paperless eBilling

Through the "My Account" portal in Summation 360, customers will be able to register for eBilling and manage their notification settings. Customers will be able to:

- Receive email bill reminders
- Opt-in/out of receiving paper bill
- Store and view current and archived bill images online. The CITY may need to contract with an outside vendor for programming or may need to have staff provide programming within the Sungard financial system in order for customers to view current and archived bill images online through the use of Summation 360 or to suppress the printing of paper bills.

Web – Mobile

Web Mobile provides a web application formatted for smartphones and tablet devices with broad mobile browser support and conforms to typical mobile touchscreen operations including navigation, screen formatting, and orientation changes that work seamlessly on mobile devices.

- Web payment interface formatted for mobile devices
- Text reminders facilitate web mobile payments
- Real-time account access and payment posting

Interactive Voice Response (IVR) / Phone Services

The Summation360 IVR module provides customers with self-service options via the telephone. The IVR allows customers to obtain general account status and balance information and to make a payment on their account. The IVR includes the following:

- Log in with account number and the numeric portion of street address
- Hear current account balance and last payment amount
- Pay bills by credit card or eCheck through Summation 360
- Real-time account access and payment posting through the API.

Customer Notifications

Summation360 includes the *alertworks™* outbound notification system enabling CITY to rapidly deliver messages via telephone, email and text message. All notification events will be created and initiated at the discretion of CITY. Standard *alertworks* features are as follows:

- Web-Based Campaign Control – An easy-to-use web interface is used for creating and managing outbound phone, text messaging, and e-mail campaigns (email broadcasts relayed through Client's SMTP server).
- Contact Sources – Ability to import contact information from multiple contact sources stored within Sungard HTE system, with user friendly field mapping interface.
- Scheduling – Notifications can be scheduled in advance to run at a set time (e.g., reminder call-outs could be set to run in the evening when people are home from work).
- Retry Attempts / Voice Mail / Alternate Content – The system includes multiple configuration settings that the CITYcan use depending on the result of the call; these include setting the number of retry attempts, detecting voice mail, leaving a message, and leaving an alternate message for voice mail.
- Message Content – Message content is created by typing in a message on web console. Message content can include account specific data "merged" into the message. Voice/phone messages can be read back using text-to-speech (TTS) or recorded voice (i.e, WAV) (Note: account specific merge values are not supported with recorded voice.)
- Reporting – *Alertworks* provides comprehensive reporting on the results of call out attempts, including the final disposition of each call that was placed (e.g. delivered to human, voicemail, busy, etc.).
- Press-2-to-Pay – Call recipients can "Press 2" from the outbound call to enter the IVR system to make a payment directly from the outbound call.
- SMS Message Delivery: TWI cannot guarantee the delivery of every text message. Deliverability and response times are dependent upon the carrier and their network.
- SMS Supported "Response" Messages: An end user can opt-out by replying with the text message, "STOP." This will block the number from receiving future messages. The user may text back "RESUME" to unblock the number. The automatic STOP and RESUME feature is not optional nor are the responses case sensitive. Alertworks will post response messages up to 5 days from the time the recipient receives the message.
- Standard and High-Volume Call-Out Capacity: The Client can make call-outs using either of two call-out capacities. Standard Capacity provides the ability to place approximately 12 simultaneous calls; High-Volume Capacity provides the ability to place hundreds of calls simultaneously.

Payment Processing

Part of the Summation360 Solution Suite, TWI Payment Processing includes the ability to securely process utility payments made to the CITY via eCheck as well as credit/debit card, including but not limited to VISA, MasterCard, Discover, and American Express via Web, IVR, and mobile payment channels. Specific terms and conditions for payment processing are defined in the Merchant Services Agreement which is attached as Appendix A. Key features provided by TWI Payment Processing Services include the following:

- Secure, encrypted bank card and ACH bank draft approvals
- One-time or recurring payments
- Detailed transaction reports, "virtual terminal" access, and tokenization for secure card-on-file transactions which meet or exceed the requirements of PCI DSS portal communications standards.
- Real-time payment posting through the API

General Summation360 Requirements

Account information and updates are made via a real-time integration with the Client's host CIS database. Real-time integration requires the CITY to acquire, install, and maintain the appropriate Application Programming Interface (API) from the Sungard HTE financial system used by the CITY. The API must be installed on a Web server within the Client's data center and connected to the Client's Database. The Web services API must be accessible to TWI's hosted platform through the Internet. Upon delivery of APIs by the CITY, TWI will conduct data validation sessions with CITY staff to ensure the APIs function as expected to support all proposed functionality. With the successful testing of the APIs, TWI's implementation efforts and coordination with the necessary CITY resources will commence. CITY understands that the timely completion of the project is contingent upon timely performance by CITY of all of CITY's obligations described in this SOW and the Task Matrix attached as Appendix E. In the event that progress on the project is slowed or halted due to a delay by CITY, project schedules may be modified by mutual agreement of CITY and TWI project resources. TWI shall not be liable for any delays or failure to perform resulting from CITY's failure to timely provide any information, content or other deliverables necessary to provide the Products and Services to CITY. CITY also accepts that availability of features outlined above may be limited or delayed by APIs and/or by TWI Product Release Schedules and that TWI reserves the right to implement features in phases as they become available. The planned implementation schedule for the CITY is outlined in Appendix E.

TERMS AND CONDITIONS

3. Penalty for Early Termination for Convenience. CITY understands that there will be significant upfront costs incurred by TWI associated with the implementation of a real-time solution integrated with the CITY's business processes. Should CITY terminate this Agreement prior to the end of the Initial Term and TWI has performed its obligations pursuant to the terms of the Agreement, the CITY shall pay a Penalty for Early Termination. If the termination by CITY occurs during the first year of the Initial Term, CITY shall pay TWI an early termination fee of Forty Thousand Dollars ($40,000.00). If the termination by CITY occurs during the second year of the Initial Term, CITY shall pay TWI Thirty Thousand Dollars ($30,000.00). UNDER NO CIRCUMSTANCE SHALL THE EARLY TERMINATION PENALTY BE ASSESSED OR PAID IF TWI HAS FAILED TO PERFORM ACCORDING TO THE TERMS OF THIS AGREEMENT, IF TWI HAS FAILED TO COMPLY WITH PCI DSS PORTAL COMMUNICATION STANDARDS, OR IF TWI IS OTHERWISE IN DEFAULT.

4. Termination.

   a. For Convenience. Either party may terminate this Agreement at any time upon thirty (30) days prior written notice to the other party. In the event of such termination, Client's entire financial obligation to TWI shall be for then accrued payments due in addition to any applicable early termination fee.

   b. Due to a Change in Fees. TWI may terminate this Agreement if TWI's ODFI (Originating Depository Financial Institution), merchant bank, non-bank credit card issuers, or related processors change their rate structure more than 5% and/or the CITY's average utility bill payment amount exceeds two hundred and ten dollars ($210.00) for six (6) consecutive months, and/or the CITY wishes to charge its customers a Technology Service Fee or other transactional fee in excess of Four Dollars and Sixty cents ($4.60).

   c. For Default. Either party may terminate this Agreement for default with thirty (30) days written notice including details of the presumed Default. The Defaulting Party will have thirty (30) days to rectify to the satisfaction of the Terminating Party.

   d. End of Contract. At the end of the contract, either through termination or expiration, TWI shall provide to the City at no cost a method of migrating or exporting all data in a usable basis. Said method and format shall be acceptable to the City.

5. Pricing / Payment Terms. CITY will pay the fees listed as follows. TWI Terms are NET 30

a. For Payments through the Summation 360 System. TWI will invoice CITY monthly for all approved payments made through the *Summation360* system at the price of Four Dollars and sixty cents ($4.60) per approved payment by credit card or debit card; and at a price of One Dollar and fifty cents ($1.50) per approved payment made by eCheck through the Summation360 System. These fees shall only be assessed on credit card payments through the Summation 360 system, debit card payments through the Summation 360 System, and eCheck payments made through the Summation 360 System. If a customer pays the CITY via credit card, debit card or eCheck but does not use the Summation 360 System, then no fee will be assessed. For purposes of this Section, "approved payment" shall mean a payment, in an amount not to exceed one thousand dollars ($1,000.00) per payment, that is not declined or otherwise rejected for payment by the customer's credit card company or bank, when a customer makes the payment using the Summation 360 system.

b. For paperless bills. TWI shall invoice CITY for paperless bills at a rate of twelve cents ($0.12) per paperless bill that is sent by CITY through the Summation 360 System.

c. For Client Notifications through the alertworks notification system. TWI will charge the CITY the following amounts: For the first seventy thousand (70,000) outbound call –out minutes and for the first seven thousand (7,000) text message transactions per year, there shall be no charge If, in any given year, usage beyond these amounts will be invoiced at eighteen cents ($0.18) cents per call-out minute and seven cents ($0.07) per text message transaction.
   - Minutes Usage: A call of thirty (30) seconds or less will be billed the same as a call of thirty (30) seconds. After the first thirty (30) seconds, calls will be billed in six (6) second increments. All call costs are rounded up to the nearest cent. There is no charge for calls that do not connect.
   - SMS Transactions: An SMS transaction represents each text message that is sent or received through the TWI SMS Gateway. TWI charges for each transaction processed at the rate defined in this SOW.
   - SMS Response Messaging: TWI counts each message received, including responses, as a transaction.
   - SMS Message Length: A standard text message is limited to 160 characters (including letters, numbers, spaces, symbols, and punctuation). Alertworks will automatically break up the message and send it in separate messages. Each message sent will count as a transaction.
   - High-Volume Call-Out Capacity Surcharge: When using High-Volume Capacity Call-Out, Outbound Call Minutes are used up at a 50% higher rate than during Standard Capacity Call-Outs. For example, a 60 second high-volume outbound call would use 90 seconds of Outbound Call Minutes.

d. For additional Services after successful deployment of Summation 360 for the CITY. If, after the CITY in its sole discretion determines that Summation 360 has been successfully deployed and implemented to the CITY's satisfaction CITY requests any additional professional services from TWI in order to deploy additional CITY services or applications, including but not limited to, new application development and enhanced support services, TWI will provide any such additional professional services at a flat rate of one hundred and seventy-five dollars ($175.00) per hour.

6. Promotion of Services. CITY is responsible for the promotion and marketing of the Summation 360 services and commits to take, at minimum, the following specific actions within ninety (90) days of Effective Date:
   a. On the paper bill, CITY will print the web address and phone number for the Summation 360 services, along with a message promoting electronic payments and paperless billing.

   b. CITY shall provide training to CITY staff on the availability and functionality of the Summation 360 service and the associated fees.

7. Hosted Subscriber Services Terms and Conditions.
   a. Network Traffic. CITY acknowledges that TWI is providing a hosted service, which means that CITY content and data will pass through hosted TWI servers that are not segregated or in a separate physical location from servers on which the content of other third parties is or will be transmitted or stored. TWI shall maintain the security of CITY content and data and that of CITY's customers that is stored in or in any way connected with TWI's hosted service or TWI's servers. TWI warrants that it will comply with all Laws, PCI DSS portal communication standards, SAS70 Auditing Standards, CITY's Red Flag Policy, and the CITY's Cloud Computing Requirements which are contained in Appendix B. If either Party believes or suspects that security has been breached or data compromised whether it be from harmful code or otherwise, the Party shall notify the Other Party of the issue or possible security breach within forty-eight (48) hours.

b. Content. CITY is and shall be solely responsible for the creation, editorial content, control, and all other aspects of content. Client represents and warrants that it has obtained (or will obtain, prior to transmission) all authorizations and permissions required to use and transmit the content over TWI's hosted products and services.

c. CITY Maintenance. CITY is responsible for, and TWI is not liable for CITY's failure in, properly configuring, developing, programming, hosting and operating CITY's hardware, software, web sites, content and all CITY's applications, and their respective telephone and Internet connections, to allow necessary access to CITY's API for use of TWI hosted products and services, and providing any connections necessary to communicate with the TWI hosted products and services.

d. No Call "Front Ending": TWI hosted IVR cannot be used to "front end" calls to the Client's live agent queue or call group. The Client must direct its customers to the IVR as an option off the Agency's phone system auto-attendant.

8. Support for Products and Services. During the Term, TWI shall be responsible for providing support to CITY according to TWI prevailing Product and Services Support Policy, attached as Appendix C, and incorporated herein by reference. CITY shall be responsible for providing support to its end users with regard to the Hosted Subscriber Services.

9. Data Security. During the Term, TWI shall be solely responsible for ensuring that its software and hosted systems remain in compliance with all requirements related to the protection of data as relates to Red Flag Rules and Payment Card Industry Data Security Standards (PCI DSS). This fact does not, however, release CITY from its own obligations relative to the FTC's Red Flag Rule and PCI DSS. TWI is responsible for the security of CITY and CITY's customer data that passes through or is stored in or on TWI's systems.

10. Red Flag Requirements. TWI agrees to comply with the CITY's Red Flag Policy and any Amendment thereto, a copy of which is attached to this Agreement as Appendix D. TWI shall provide CITY with a copy of its existing Red Flag policies and procedures, and shall promptly provide copies of any changes to its Red Flag policies and procedures.

    TWI shall comply with the CITY's red flag policy and timely report any Red Flags to the CITY's Program Administrator. Said report shall include Red Flags detected by TWI and TWI's response to the Red Flags so detected. Pursuant to the City's Red Flag Policy, TWI shall store the documents and files in a secure manner so as to be accessible only by approved TWI and city personnel.

11. Critical Applications and Emergency Uses. Client acknowledges and agrees that the Products and Services are not designed, intended, authorized or warranted to be suitable for hosting life-support applications or other critical applications where the failure or potential failure of the Products and Services can cause injury, harm, death, or other grave problems, including, without limitation, loss of aircraft control, hospital life-support systems, delays in getting medical care or other emergency services. If the products and services are used in emergency situations for outbound notifications, then the products and services are intended to only increase the notice which will be given. There is and cannot be any guarantee that all persons intended to be contacted will be contacted. TWI accepts no responsibility for any failure of the products and services to contact any person(s) and is not responsible for any damage or injury which results from any failure to contact anyone.

12. Force Majeure. Except for CITY's obligations to pay money, neither party shall be deemed to be in breach of this Agreement for any failure or delay in performance caused by reasons beyond its reasonable control, including but not limited to acts of God, earthquakes, strikes, war, crime, terrorism, shortages of materials, internet, power or telecommunications failures, etc.

13. Copyright / Intellectual Property. All right, title, and interest, including all intellectual property rights in the products and services of TWI, and any updates, upgrades or modifications by TWI thereof, or in any ideas, know-how, and programs developed by TWI during the course of performance of this Agreement shall remain the property of TWI. All right, title, and interest in any content communicated via TWI infrastructure through use of the products and services shall remain the sole property of CITY. All products and service provided under this agreement are owned by TWI and are protected by United States copyright laws and applicable international treaties and/or conventions. The products and services, and any and all modifications and improvements thereto and derivative works thereof created by TWI, shall remain the exclusive property of TWI, and Client shall have no right, title or interest therein whatsoever.

14. Compliance with Merchant Agreement. Each Party agrees to comply with the terms of the Merchant Agreement, attached as Appendix A and incorporated herein by reference.

15. TWI's Representations and Warranties. TWI represents and warrants as follows:

a. TWI is a corporation, duly organized, validly existing, and in good standing under the laws of the State of Virginia, and authorized to conduct business in Missouri;

b. TWI has the power and authority to enter into and perform this Agreement and is not prohibited from entering into this Agreement or discharging and performing all covenants and obligations on its part to be performed under and pursuant to this Agreement;

c. The execution and delivery of this Agreement, the consummation of the transactions contemplated herein and the fulfillment of and compliance by TWI with the provisions of this Agreement will not conflict with or constitute a breach of or a default under or require any consent, license or approval that has not been obtained pursuant to any of the terms, conditions or provisions of any law, rule or regulation, any order, judgment, writ, injunction, decree, determination, award or other instrument or legal requirement of any court or other agency of government, the documents of formation of TWI or any contractual limitation, restriction or outstanding trust indenture, deed of trust, mortgage, loan agreement, lease, other evidence of indebtedness or any other agreement or instrument to which TWI is a party or by which it or any of its property is bound and will not result in a breach of or a default under any of the foregoing;

d. With the exception of the approval by its board of directors (or equivalent governing body), TWI has taken all such action as may be necessary or advisable and proper to authorize this Agreement, the execution and delivery hereof, and the consummation of transactions contemplated hereby;

e. There is no bankruptcy, insolvency, reorganization or receiverships pending or being contemplated by TWI, or to its knowledge threatened against TWI;

f. To the TWI's knowledge, there are no actions, proceedings, judgments, rulings or orders issued by, or pending before any court or other governmental body that would materially adversely affect TWI's ability to perform its obligations under this Agreement; and

g. Beyond the requirements provided by Columbia and TWI responses to same as documented in Appendix F, TWI does not warrant that the products and services shall meet all of CITY's requirements, or that the use of the products and services shall be uninterrupted or error-free.

h. This Agreement is a legal, valid and binding obligation of TWI enforceable in accordance with its terms, except as limited by laws of general applicability limiting the enforcement of creditor's right or by the exercise of judicial discretion in accordance with general principles of equity.

16. TWI's Covenants.

a. TWI covenants that TWI shall at all times comply with the terms of this Agreement, Good Financial Industry and Accounting Practices, Applicable Laws, CITY's Red Flag Policy, PCI DSS portal communication standards, and SAS70 auditing standards.

b. TWI further covenants that any data from the CITY, its employees or customers or derived therefrom shall be stored in the United States of America. The data or any information derived therefrom shall not be transferred, moved, or stored to or at any location outside the United States of America. All such data and any information derived therefrom shall be confidential and proprietary information belonging to either the CITY or its customers. TWI shall not sell or give away any such CITY data or information derived therefrom.

17. Successors and Assigns; Assignment. This Agreement shall inure to the benefit of and shall be binding upon the Parties and their respective successors and assigns. This Agreement shall not be assigned or transferred by either Party without the prior written consent of the other Party.

18. Notices. Each notice, request, demand, statement or routine communication required or permitted under this Agreement, or any notice or communication that either Party may desire to deliver to the other, shall be in writing and shall be considered delivered effective:

a. when verified by written receipt if sent by personal courier, overnight courier, or mail; or

b. when verified by automated receipt or electronic logs if sent by facsimile or email. Each such notice must be addressed to the other Party at its address indicated below or at such other address and by means as either Party may designate for itself in a written notice to the other Party in accordance with this Section.

If to TWI: Tele-Works, Inc.

P.O. Box M

Blacksburg, VA 24060

Attn: Andy Hall

Telephone: (540) 951-6464

Facsimile: (540) 951-4016

Email: ahall@summation360.com

If to CITY: City of Columbia

P.O. Box 6015

Columbia, Missouri 65205

Attention: Will Hobart

Telephone: (573) 874-7687

Facsimile: (573) 874-7761

Email: wahobart@gocolumbiamo.com

19. Amendments. This Agreement shall not be modified nor amended unless such modification or amendment shall be in writing and signed by authorized representatives of both Parties.

20. Audit. Each Party has the right, at its sole expense and during normal working hours, to examine the records of the other Party to the extent reasonably necessary to verify the accuracy of any statement, charge or computation made pursuant to this Agreement. If any such examination reveals any inaccuracy in any statement, the necessary adjustments in such statement and the payments thereof will be made

21. Waivers. Failure to enforce any right or obligation by any Party with respect to any matter arising in connection with this Agreement shall not constitute a waiver as to that matter nor to any other matter. Any waiver by any Party of its rights with respect to a default under this Agreement or with respect to any other matters arising in connection with this Agreement must be in writing. Such waiver shall not be deemed a waiver with respect to any subsequent default or other matter.

22. Severability. If any of the terms of this Agreement are finally held or determined to be invalid, illegal or void, all other terms of the Agreement shall remain in effect; provided that the Parties shall enter into negotiations concerning the terms affected by such decision for the purpose of achieving conformity with requirements of any Applicable Law and the intent of the Parties.

23. Governing Law And Venue. This Agreement shall be governed, interpreted, and enforced in accordance with the laws of the State of Missouri and/or the laws of the United States, as applicable. The venue for all litigation arising out of, or relating to this contract document, shall be in the United States Western District of Missouri. The Parties hereto irrevocably agree to submit to the exclusive jurisdiction of the federal courts in the State of Missouri. The Parties agree to waive any defense of forum non conveniens.

24. No Third-Party Beneficiaries. This Agreement is intended solely for the benefit of the Parties hereto and nothing contained herein shall be construed to create any duty to, or standard of care with reference to, or any liability to, or any benefit for, any Person not a Party to this Agreement.

25. Employment of Unauthorized Aliens Prohibited. TWI agrees to comply with Missouri State Statute Section 285.530 in that TWI shall not knowingly employ, hire for employment, or continue to employ an unauthorized alien to perform work within the State of Missouri. As a condition for the award of this contract, TWI shall, by sworn affidavit and provision of documentation, affirm its enrollment and participation in a federal work authorization program with respect to the employees working in connection with the contracted services. TWI shall also sign an affidavit affirming that it does not knowingly employ any person who is an unauthorized alien in connection with the contracted services.

26. Insurance Requirements.

    a. TWI agrees to maintain, on a primary basis and at its sole expense, at all times during the life of this contract the following insurance coverages, limits, including endorsements described herein. The requirements contained herein, as well as CITY's review or acceptance of insurance maintained by TWI is not intended to and shall not in any manner limit or qualify the liabilities or obligations assumed by TWI under this contract.

    b. Commercial General Liability. TWI agrees to maintain Commercial General Liability at a limit of liability not less than $2,000,000.00 combined single limit for any one occurrence covering both bodily injury and property damage, including accidental death. Coverage shall not contain any endorsement(s) excluding nor limiting Contractual Liability or Cross Liability.

c. Professional Liability. TWI agrees to maintain Professional (Errors & Omissions) Liability at a limit of liability not less than $2,000,000.00 per claim and $2,000,000.00 aggregate. For policies written on a "Claims-Made" basis, TWI agrees to maintain a Retroactive Date prior to or equal to the effective date of this contract. In the event the policy is canceled, non- renewed, switched to an Occurrence Form, retroactive date advanced; or any other event triggering the right to purchase a Supplemental Extended Reporting Period (SERP) during the life of this contract, TWI agrees to purchase a SERP with a minimum reporting period not less than two (2) years. The requirement to purchase a SERP shall not relieve TWI of the obligation to provide replacement coverage.

d. Business Automobile Liability. TWI agrees to maintain Business Automobile Liability at a limit of liability not less than $2,000,000.00 combined single limit for any one occurrence and not less than $150,000.00 per individual, covering both bodily injury, including accidental death, and property damage, to protect themselves from any and all claims arising from the use of the TWI's own automobiles, and trucks; hired automobiles, and trucks; and automobiles both on and off the site of work. Coverage shall include liability for Owned, Non-Owned & Hired automobiles. In the event TWI does not own automobiles, TWI agrees to maintain coverage for Hired & Non-Owned Auto Liability, which may be satisfied by way of endorsement to the Commercial General Liability policy or separate Business Auto Liability policy.

e. Workers' Compensation Insurance & Employers' Liability. TWI agrees to take out and maintain during the life of this contract, Employers' Liability and Workers' Compensation Insurance for all of their employees employed at the site of the work, and in case any work is sublet, the TWI shall require the subcontractor similarly to provide Workers' Compensation Insurance for all the latter's employees unless such employees are covered by the protection afforded by the TWI. Workers' Compensation coverages shall meet Missouri statutory limits. Employers' Liability minimum limits shall be $500,000.00 each employee, $500,000.00 each accident and $500,000.00 policy limit. In case any class of employees engaged in hazardous work under this contract is not protected under the Workers' Compensation Statute, TWI shall provide and shall cause each subcontractor to provide Employers' Liability Insurance for the protection of their employees not otherwise protected.

f. Excess/Umbrella Liability. The above liability limits may be satisfied by any combination of primary and excess/umbrella liability policies.

g. Additional Insured. TWI agrees to endorse CITY as an Additional Insured with a CG 2026 Additional Insured – Designated Person or Organization endorsement, or similar endorsement, to the Commercial General Liability. The Additional Insured shall read "City of Columbia."

h. Waiver of Subrogation. TWI agrees by entering into this contract to a Waiver of Subrogation for each required policy herein except professional liability. When required by the insurer, or should a policy condition not permit TWI to enter into an pre-loss agreement to waive subrogation without an endorsement, then TWI agrees to notify the insurer and request the policy be endorsed with a Waiver of Transfer of Rights of Recovery Against Others, or its equivalent. This Waiver of Subrogation requirement shall not apply to any policy, which includes a condition specifically prohibiting such an endorsement, or voids coverage should TWI enter into such an agreement on a pre-loss basis.

i. Certificate(s) of Insurance. TWI agrees to provide CITY with Certificate(s) of Insurance evidencing that all coverages, limits and endorsements required herein are maintained and in full force and effect. Said Certificate(s) of Insurance shall include a minimum thirty (30) day endeavor to notify due to cancellation or non-renewal of coverage. The Certificate(s) of Insurance shall name the City as additional insured in an amount as required in this contract and contain a description of the project or work to be performed.

j. Right to Revise or Reject. CITY reserves the right, but not the obligation, to review and revise any insurance requirement, not limited to limits, coverages and endorsements based on insurance market conditions affecting the availability or affordability of coverage; or changes in the scope of work / specifications affecting the applicability of coverage. Additionally, the CITY reserves the right, but not the obligation, to review and reject any insurance policies failing to meet the criteria stated herein or any insurer providing coverage due of its poor financial condition or failure to operating legally.

27. HOLD HARMLESS AGREEMENT. To the fullest extent not prohibited by law, TWI shall indemnify and hold harmless the City of Columbia, its directors, officers, agents and employees from and against all claims, damages, losses and expenses (including but not limited to attorney's fees) to the extent caused by any negligent act or failure to act, or willful misconduct, of TWI, of any subcontractor (meaning anyone, including but not limited to contractors having a contract with TWI or a subcontractor for part of the services), of anyone directly or indirectly employed by TWI or by any subcontractor, or of anyone for whose acts the TWI or its subcontractor may be liable, in connection with providing these services except as provided in this Agreement. This provision

does not, however, require TWI to indemnify, hold harmless or defend the City of Columbia from its own negligence, except as set out herein.

28. Professional Oversight Indemnification. TWI understands and agrees that CITY has contracted with TWI based upon TWI's representations that TWI is a skilled professional and fully able to provide the services set out in this Agreement. In addition to any other indemnification set out in this Agreement, TWI agrees to defend, indemnify and hold and save harmless the CITY from any and all claims, settlements and judgments whatsoever arising out of the CITY's alleged negligence in hiring or failing to properly supervise TWI. The insurance required by this Agreement shall include coverage which shall meet TWI's obligations to indemnify the CITY as set out above and the CITY shall be named as co-insured for such insurance.
29. General Laws. TWI shall comply with all federal, state, and local Laws, statutes, ordinances, and rules and regulations.
30. Nature of City's Obligations. The obligations of CITY under this Agreement, which require the expenditure of funds, shall be conditional obligations, subject to the availability of funds appropriated for the purpose.
31. Entire Agreement. This Agreement shall supersede all other prior and contemporaneous understandings or agreements, both written and oral, between the Parties relating to the subject matter of this Agreement.

IN WITNESS WHEREOF the Parties have executed this Agreement in the manner appropriate to each on the date set forth above.

Tele-Works Incorporated

_____

By: Andy Hall, COO

ATTEST:

_____

Signature

Name:_____

Title:_____

CITY OF COLUMBIA, MISSOURI

_____

By: Mike Matthes, City Manager

ATTEST:

_____

Sheela Amin, City Clerk

APPROVED AS TO FORM:

_____

Fred Boeckmann, City Counselor

Client Billing/Invoicing Information:

_____ Billing Contact

_____ Primary Email Address

_____ Secondary Email Address

_____ Client Billing Address (if hard copy invoices also desired)

_____

_____

MERCHANT AGREEMENT

1 **Requirements.**

The following rules are requirements strictly enforced by Visa, MasterCard and Discover Network: (a) You cannot establish minimum or maximum amounts as a condition for accepting a Card, except that for Discover Network transactions, you may limit the maximum amount a Discover Network Cardholder may spend if, and only if, you have not received a positive authorization response from the Card Issuer; (b) You cannot impose a surcharge or fee for accepting a Card; (c) You cannot establish any special conditions for accepting a Card; (d) You cannot establish procedures that discourage, favor or discriminate against the use of any particular Card. However, you may choose not to accept either U.S. issued Debit Cards or U.S. issued Credit Cards under the terms described in Section 2; (e) You cannot require the Cardholder to supply any personal information (e.g., home or business phone number; home or business address; or driver's license number) unless instructed by the Authorization Center. The exception to this is for a mail/telephone/Internet order or delivery-required transaction, and zip code for a card-present key-entered transaction in order to obtain an Address Verification ("AVS"). Any information that is supplied by the Cardholder must not be in plain view when mailed; (f) Any tax required to be collected must be included in the total transaction amount and not collected in cash; (g) You cannot submit any transaction representing the refinance or transfer of an existing Cardholder obligation deemed uncollectible; (h) You cannot submit a transaction or sale that has been previously charged back; (i) You must create a Sales or Credit Draft for each Card transaction and deliver at least one copy of the Sales or Credit Draft to the Cardholder; (j) You cannot submit a transaction or sale to cover a dishonored check; (k) If you accept Card checks, your Card check acceptance policy must treat the acceptance of checks from all payment card brands that you accept equally. (e.g., if you accept MasterCard, Visa and Discover Network, your check acceptance policy must treat checks for all three payment card brands equally). You should handle these Card checks like any other personal check drawn upon a bank in the United States; (l) Failure to comply with any of the Association Rules may result in fines or penalties.

2 **Card Acceptance.** If you have indicated either in the Application or by registering with us at least thirty (30) days in advance that, as between Non-PIN Debit Card transactions and Credit Card transactions, you will limit your acceptance to either (i) only accept Non-PIN Debit transactions; or (ii) only accept Credit Card transactions, then the following terms in this Section 2 will apply:

2.1 You will be authorized to refuse to accept for payment either Non-PIN Debit Cards or Credit Cards that are issued within the United States. You will, however, continue to be obligated to accept all foreign issued Credit or Debit Cards issued by MasterCard, Visa or Discover Network so long as you accept any type of MasterCard, Visa or Discover Network branded Card.

2.2 While many Debit Cards include markings indicating debit (such as "Visa Checkcard, Visa Buxx, Gift Card, DEBIT, or Mastermoney), many Debit Cards do not include any such markings and will not have such markings until January 2007. It will be your responsibility to determine at the point of sale whether a Card is of a type that you have indicated that you will accept. You agree to institute appropriate systems and controls to limit your acceptance to the Card types indicated. You may purchase a table of ranges of numbers currently associated with Debit Card transactions upon execution of confidentiality/non-disclosure agreements required by the Associations. You will be responsible for updating your systems to utilize such tables and to obtain updated tables.

2.3 To the extent that you inadvertently accept a transaction that you are not registered to accept, such transaction will downgrade to a Non-Qualified Credit Transaction and the Discount Rate that will be applied to the transaction will be your Non-Qualified Rate.

2.4 Based upon your choice to accept only the Card types indicated in the application you must remove from your premises any existing signage indicating that you accept all Visa, MasterCard or Discover Network Cards and use approved specific signage reflecting your policy of accepting only Non-PIN Debit or Credit Cards.

2.5 Even if you elect not to accept Non-PIN Debit Card transactions as provided above, you may still accept PIN Debit Card transactions if you have signed up for PIN Debit Card Services. The terms in Section 22 shall apply to such services.

3 **Deposits of Principals.** Owners, partners, officers and employees of your business establishment, and the guarantors who signed the Application, are prohibited from submitting Sales Drafts or Credit Drafts transacted on their own personal Cards, other than transactions arising from bona fide purchases of goods or services in the ordinary course of your business. Such use in violation of this Section 3 is deemed a cash advance, and cash advances are prohibited.

4 **Cash Payments by and Cash Disbursements to Cardholders.** You must not accept any direct payments from Cardholders for charges of merchandise or services which have been included on a Sales Draft; it is the right of the Card Issuer to receive such payments. You may not make any cash disbursements or cash advances to a Cardholder as part of a Card transaction unless you are a financial institution with express authorization in writing in advance from Servicers.

5 **Data Security**

THE FOLLOWING IS IMPORTANT INFORMATION REGARDING THE PROTECTION OF CARDHOLDER DATA. PLEASE REVIEW CAREFULLY AS FAILURE TO COMPLY CAN RESULT IN SUBSTANTIAL FINES AND LIABILITIES FOR UNAUTHORIZED DISCLOSURE AND TERMINATION OF THIS AGREEMENT.

5.1 Payment Card Industry Data Security Standards (PCI DSS). Visa, MasterCard, American Express, Discover Network and JCB aligned data security requirements to create a global standard for the protection of Cardholder data. The resulting Payment Card Industry Data Security Standards (PCI DSS) defines the requirements with which all entities that store, process, or transmit payment card data must comply. PCI DSS is the name used to identify those common data security requirements. The Cardholder Information Security Program (CISP) is Visa USA's data security program, the Site Data Protection (SDP) program is MasterCard's data security program and Discover Network Information Security and Compliance (DISC) is Discover Network's data security program, each based on the PCI DSS and industry aligned validation requirements. PCI DSS compliance validation is focused on any system(s) or system component(s) where Cardholder data is retained, stored, or transmitted, including:

- All external connections into your network (i.e., employee remote access, third party access for processing, and maintenance);
- All connections to and from the authorization and settlement environment (i.e., connections for employee access or for devices such as firewalls, and routers) ; and
- Any data repository outside of the authorization and settlement environment.

The Associations or we may impose fines or penalties, or restrict you from accepting Cards if it is determined that you are not compliant with the applicable data security requirements. We may, in our sole discretion, suspend or terminate Card processing Services under your Merchant Agreement for any actual or suspected data security compromise.

Detailed information about PCI DSS compliance can be found at the PCI DSS Council's website: www.pcisecuritystandards.org.

Detailed information about Visa's CISP program can be found at Visa's CISP website: www.visa.com/cisp.

Detailed information about MasterCard's SDP program can be found at the MasterCard SDP website: http://www.mastercard.com/us/merchant/security/sdp_program.html

Detailed information about DISC can be found at Discover Network's DISC website: http://www.discovernetwork.com/fraudsecurity/disc.html.

5.2 You must comply with the data security requirements shown below (Where Applicable):

(a) You must install and maintain a secure network firewall to protect data across public networks; (b) You must encrypt stored data and data sent across networks; (c) You must use and regularly update anti-virus software and keep security patches up-to-date; (d) You must restrict access to data by business "need to know", assign a unique ID to each person with computer access to data and track access to data by unique ID; (e) Don't use vendor-supplied defaults for system

passwords and other security parameters; (f) You must regularly test security systems and processes; (g) You must maintain a policy that addresses information security for employees and contractors; (h) You must restrict physical access to Cardholder information; (i) You may not transmit Cardholder account numbers to Cardholders for Internet transactions; (j) You cannot store or retain Card Validation Codes (three-digit values printed in the signature panel of most Cards, and a four-digit code printed on the front of an American Express Card); (k) You cannot store or retain Magnetic Stripe data, PIN data or AVS data. Only Cardholder account number, Cardholder Name and Cardholder expiration date can be retained subsequent to transaction authorization; (l) You must destroy or purge all Media containing obsolete transaction data with Cardholder information; (m) You must keep all systems and Media containing Card account, Cardholder, or transaction information (whether physical or electronic) in a secure manner so as to prevent access by, or disclosure to any unauthorized party; and (n) For Internet transactions, copies of the transaction records may be delivered to Cardholders in either electronic or paper format.

5.3 You may be subject to ongoing validation of your compliance with PCI DSS standards. Furthermore, we retain the right to conduct an audit (at your expense if such audit discovers noncompliance with any of your obligations as set forth in this Paragraph 5), performed by us or a third party designated by us to verify your compliance, or that of your agents or third party providers, with security procedures and these Operating Procedures.

5.4 In the event that transaction data suspected of having been accessed or retrieved by any unauthorized person or entity, contact us immediately and in no event more than 24 hours after becoming aware of such activity.

5.5 You must, at your own expense (i) perform or cause to be performed an independent investigation (including a forensics analysis) of any data security breach of Card or transaction data, (ii) perform or cause to be performed any remedial actions recommended by any such investigation, and (iii) cooperate with us in the investigation and resolution of any security breach.

5.6 **Required Information for Discover Network Security Breaches.** For security breaches involving Discover Network transactions and/or track data, you must provide us and/or Discover Network with the following information to the extent it is known to you or in your possession and/or control: (i) the date of breach; (ii) details concerning the data compromised (e.g., account numbers and expiration dates, Cardholder names and addresses, etc.); (iii) the method of such breach; (iv) your security personnel contacts; (v) the name of any person (including law enforcement) assisting you with your investigation of such breach; and (vi) any other information which we reasonably request from you concerning such breach, including forensics reports. You shall provide such information as soon as practicable, and the items listed in (i)-(v) shall be provided to us in any event within 48 hours of your initial notification to us of the breach. Discover Network reserves the right to conduct on-site visits to ensure compliance with its requirements.

5.7 **Third Parties.** The data security standards set forth above also apply to any agent or third party provider that you may use to store, process or transmit Cardholder data. In addition, such agents or third party providers must be registered with the applicable Association. Therefore, you must: (a) Notify us in writing of any agent or third party processor that engages in, or proposes to engage in, the storing, processing or transmitting of Cardholder data on your behalf, regardless of the manner or duration of such activities and; (b) Ensure that all such agents or third party processors are (i) registered with the applicable payment card brands; and (ii) comply with all applicable data security standards, including, without limitation, the PCI DSS.

You are solely responsible for the compliance of any and all third parties that are given access by you, to Cardholder data, and for any third party software that you may use.

6 Credit Card Operating Procedures; Association Rules

6.1 You agree to follow all requirements of this Agreement in connection with each Card transaction and to comply with all applicable Association Rules. From time to time, we may amend the Operating Procedures, by providing you with at least 20 days' prior written notice, and those provisions will be deemed incorporated into this Agreement. However, for changes in the Association Rules or for security reasons, certain changes in Card procedures may become effective on shorter notice.

6.2 Our Agreement with you includes Operating Procedures which contain procedures, instructions and other directives relating to Card transactions. If you fail to follow any of the provisions of the Operating Procedures, you may incur certain liabilities or we may terminate the Agreement. You will receive the Operating Procedures at the time you sign your Merchant Agreement and you may request additional copies at anytime from your sales representative or by calling customer service. You agree that if you process Card transactions, you will comply with the Operating Procedures for all transactions you process. The current Operating Procedures are also available online at http://www.paypros.com/fdmsdocs/ppiopguide0408.pdf. If there are any inconsistencies between the Merchant Application and Agreement and the Operating Procedures, the Merchant Application and Agreement will govern. If any part of the Merchant Agreement is not enforceable, the remaining provisions shall remain valid and enforceable.

7 Settlement

Your funds for MasterCard/Visa/Discover Network transactions will be processed and transferred to your financial institution within two (2) Business Days from the time a Batch is received by Processor if your financial institution is the Bank. If your financial institution is not the Bank, your MasterCard/Visa/Discover Network transactions will be processed via the Federal Reserve within two (2) Business Days from the time a batch is received by Processor. The Federal Reserve will transfer such amounts to your financial institution.

8 Settlement Of Card Transactions

8.1 We will only be required to settle Card transactions for Card types specified in your Application. Promptly after presentment of Sales Drafts pursuant to the Operating Procedures, we will initiate a transfer of the applicable settlement funds to you.

8.2 All settlements for Visa, MasterCard and Discover Network Card transactions will be net of Credits/refunds, adjustments, applicable discount fees when due, Chargebacks and any other amounts then due from you. We may also set off from any payments otherwise due, any amounts owed to our affiliates (and/or affiliates of Bank) whether or not arising out of or related to this Agreement.

8.3 All Credits to your Settlement Account or other payments to you are provisional and are subject to, among other things, our final audit, Chargebacks (including our related losses), fees and fines imposed by the Associations. You agree that we may debit or credit your Settlement Account for any deficiencies, overages, fees and pending Chargebacks, or may deduct such amounts from settlement funds due to you. Alternatively, we may elect to invoice you for any such amounts, net due 30 days after the invoice date or on such earlier date as may be specified.

8.4 We will not be liable for any delays in receipt of funds or errors in debit and Credit entries caused by third parties including but not limited to any Association or your financial institution.

8.5 In addition to any other remedies available to us under this Agreement, you agree that should any Event of Default (see Section 17) occur, we may, with or without notice, change processing or payment terms and/or suspend Credits or other payments of any and all funds, money and amounts now due or hereafter to become due to you pursuant to the terms of this Agreement, until we have had reasonable opportunity to investigate such event.

9 INTENTIONALLY OMITTED

10 Fees; Adjustments; Collection Of Amounts Due

10.1 You acknowledge that for Visa, MasterCard and Discover transactions, we will process your Card transactions at the Qualified Discount Rate only when your transactions meet certain criteria set by the applicable Association and us. When your Card transactions fail to meet those qualification criteria, we will process your transactions at the higher Non-Qualified Discount Rate (or, in certain circumstances, at an intermediate Mid-Qualified Discount Rate) indicated in this Merchant Application and Agreement. The current requirements for the Qualified Discount Rate and, if applicable, the Mid- and Non-Qualified Discount Rates will be given to you upon acceptance of your application and are also available for your review by asking your sales representative or calling customer service.

10.2 All authorization fees will be charged for each transaction that you attempt to authorize. All capture fees will be charged for each transaction that you transmit to us for settlement.

10.3 The fees for Services set forth in this Agreement are based upon assumptions associated with the anticipated annual volume and average transaction size for all Services as set forth in this Agreement and your method of doing business. If the actual volume or average transaction size are in substantial part not as expected or if you significantly alter your method of doing business, we may adjust your discount fee and transaction fees without prior notice.

10.4 The fees for Services set forth in this Agreement may be adjusted to reflect increases or decreases by Associations in interchange, assessments and other Association fees or to pass through increases charged by third parties for on-line communications and similar items. All such adjustments shall be your responsibility to pay and shall become effective upon the date any such change is implemented by the applicable Association or third party.

10.5 Subject to Section 15.3, we may also increase our fees for Services for any other reason by notifying you 30 days prior to the effective date of any such change.

10.6 If you receive settlement funds by wire transfer, we may charge a wire transfer fee per wire.

10.7 To the extent the Automated Clearing House ("ACH") settlement process is used to effect debits or Credits to your Settlement Account, you agree to be bound by the terms of the operating rules of the National Automated Clearing House Association, as in effect from time to time. You hereby authorize us to initiate credit and debit entries and adjustments to your account through the ACH settlement process and/or through direct instructions to the financial institution where your Settlement Account is maintained for amounts due under this Agreement and under any agreements with us or our affiliates for any related services, as well as for any credit entries in error. You hereby authorize the financial institution where your Settlement Account is maintained to effect all such debits and credits to your account. This authority will remain in full force and effect until we have given written notice to the financial institution where your Settlement Account is maintained that all monies due under this Agreement and under any other agreements with us or our affiliates for any related services have been paid in full.

10.8 You agree to pay any fines imposed on us by any Association resulting from Chargebacks and any other fees or fines imposed by an Association with respect to your acts or omissions. You are also responsible for any fines or fees imposed on us as a result of acts or omissions by your agents or third parties.

10.9 If your Chargeback percentage for any type of business conducted by you exceeds the estimated industry Chargeback percentage for such business types, you shall, in addition to the Chargeback fees and any applicable Chargeback handling fees or fines, pay us an excessive Chargeback fee for all Chargebacks occurring in such month in such types (s) of business. Each estimated industry Chargeback percentage is subject to change from time to time by us in order to reflect changes in the industry Chargeback percentages reported by Visa, MasterCard or Discover Network. Your Chargeback Percentage will be calculated as the larger of (a) the total Visa, MasterCard and Discover Network Chargeback items in any type of business in any calendar month divided by the number of Visa, MasterCard and Discover Network transactions in that line of business submitted that month; or (b) the total dollar amount of Visa, MasterCard and Discover Network Chargebacks in any type of business received in any calendar month divided by the total dollar amount of your Visa, MasterCard and Discover Network transactions in that line of business submitted in that month.

10.10 If you believe any adjustments should be made with respect to your Settlement Account, you must notify us in writing within 45 days after any debit or Credit is or should have been effected. If you notify us after such time period, we may, in our discretion, assist you, at your expense, in investigating whether any adjustments are appropriate and whether any amounts are due to or from other parties, but we shall not have any obligation to investigate or effect any such adjustments. Any voluntary efforts by us to assist you in investigating such matters shall not create any obligation to continue such investigation or any future investigation.

11 Chargebacks

11.1 You shall be responsible for reimbursing us for all transactions you submit that are charged back. See the Operating Procedures for additional information regarding Chargebacks and Chargeback procedures.

11.2 You shall reimburse us for any Chargebacks, return items, or other losses resulting from your failure to produce a Card transaction record requested by us within the applicable time limits.

12 Representations; Warranties; Limitations On Liability; Exclusion Of Consequential Damages

12.1 Without limiting any other warranties hereunder, you represent and warrant as to each Card transaction submitted under our Agreement that:

12.1.1 The Card transaction represents a bona fide sale/rental of merchandise or services not previously submitted;

12.1.2 The Card transaction represents an obligation of the Cardholder for the amount of the Card transaction;

12.1.3 The amount charged for the Card transaction is not subject to any dispute, setoff or counterclaim;

12.1.4 The Card transaction amount is only for the merchandise or services (including taxes, but without any surcharge) sold or rented and, except for any delayed delivery or advance deposit Card transactions expressly authorized by this Agreement, the merchandise or service was actually delivered to or performed for the person entering into the Card transaction simultaneously upon your accepting and submitting the Card transaction for processing;

12.1.5 The Card transaction does not represent the refinancing of an existing obligation of the Cardholder (including any obligation otherwise owed to you by a Cardholder or arising from the dishonor of a personal check);

12.1.6 You have no knowledge or notice of any fact, circumstances or defense which would indicate that the Card transaction was fraudulent or not authorized by the Cardholder or which would otherwise impair the validity or collectibility of the Cardholder's obligation arising from such Card transaction or relieve the Cardholder from liability with respect thereto;

12.1.7 The Card transaction submitted to us was entered into by you and the Cardholder;

12.1.8 The Card transaction was made in accordance with this Agreement, the Association Rules and the Operating Procedures; and

12.1.9 The Card transaction is not a payment for a product or service that violates federal, state or local law in any jurisdiction that may be applicable.

12.2 THIS AGREEMENT IS A SERVICE AGREEMENT. WE DISCLAIM ALL REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, MADE TO YOU OR ANY OTHER PERSON, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES REGARDING QUALITY, SUITABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR OTHERWISE OF ANY SERVICES OR ANY GOODS PROVIDED INCIDENTAL TO THE SERVICES PROVIDED UNDER THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, ANY SERVICES OR ANY GOODS PROVIDED BY A THIRD PARTY.

12.3 IN NO EVENT SHALL EITHER PARTY, OR THEIR AFFILIATES OR ANY OF THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, AGENTS OR SUBCONTRACTORS, BE LIABLE UNDER ANY THEORY OF TORT, CONTRACT, STRICT LIABILITY OR OTHER LEGAL THEORY FOR LOST PROFITS, LOST REVENUES, LOST BUSINESS OPPORTUNITIES, EXEMPLARY, PUNITIVE, SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES, EACH OF WHICH IS HEREBY EXCLUDED BY AGREEMENT OF THE PARTIES, REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE OR WHETHER ANY PARTY OR ANY ENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. CLIENT ACKNOWLEDGES AND AGREES THAT PAYMENT OF ANY EARLY CANCELLATION FEE OR LIQUIDATED DAMAGES AS PROVIDED ELSEWHERE IN THIS AGREEMENT SHALL NOT BE PROHIBITED BY THIS PARAGRAPH.

12.4 NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY (INCLUDING BUT NOT LIMITED TO SECTIONS 12.5 or 20), OUR CUMULATIVE LIABILITY FOR ALL LOSSES, CLAIMS, SUITS, CONTROVERSIES, BREACHES OR DAMAGES

FOR ANY CAUSE WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, THOSE ARISING OUT OF OR RELATED TO THIS AGREEMENT) AND REGARDLESS OF THE FORM OF ACTION OR LEGAL THEORY SHALL NOT EXCEED, (I) $50,000; OR (II) THE AMOUNT OF FEES RECEIVED BY US PURSUANT TO THE AGREEMENT FOR SERVICES PERFORMED IN THE IMMEDIATELY PRECEDING 12 MONTHS, WHICHEVER IS LESS.

12.5 NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY (INCLUDING BUT NOT LIMITED TO SECTION 20), OUR LIABILITY FOR ANY DELAY IN FUNDING TRANSACTIONS TO YOU FOR ANY REASON WILL BE LIMITED TO INTEREST COMPUTED FROM THE DATE THAT YOU SUBMIT THE TRANSACTION TO THE DATE THAT WE FUND THE TRANSACTION AT THE RATE OF THE FEDERAL FUNDS, AS ESTABLISHED BY THE FEDERAL RESERVE BOARD FROM TIME TO TIME, LESS ONE PERCENT (1%).

12.6 NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, BANK IS NOT RESPONSIBLE, AND SHALL HAVE NO LIABILITY, TO YOU IN ANY WAY WITH RESPECT TO DISCOVER NETWORK CARD, AMERICAN EXPRESS CARD, JCB CARD, PIN DEBIT CARD, AND ELECTRONIC BENEFITS TRANSFER TRANSACTIONS, TELECHECK CHECK SERVICES, TRS COLLECTION SERVICES, GIFT CARD SERVICES, AND TRANSACTIONS INVOLVING CARDS FROM OTHER NON-BANK CARD ASSOCIATIONS SUCH AS VOYAGER FLEET SYSTEMS, INC., WRIGHT EXPRESS CORPORATION AND WRIGHT EXPRESS FINANCIAL SERVICES CORPORATION.

13 **Confidentiality**

13.1 Unless you obtain consents from us and each applicable Association, Card Issuer and Cardholder, you must not use, disclose, store, sell or disseminate any Cardholder information obtained in connection with a Card transaction (including the names, addresses and Card account numbers of Cardholders) except for purposes of authorizing, completing and settling Card transactions and resolving any Chargebacks, Retrieval Requests or similar issues involving Card transactions, other than pursuant to a court or governmental agency request, subpoena or order. You shall use proper controls for and limit access to, and render unreadable prior to discarding, all records containing Cardholder account numbers and Card imprints. You may not retain or store Magnetic Stripe data or Card Validation Codes after a transaction has been authorized. If you store any electronically captured signature of a Cardholder, you may not reproduce such signature except upon our specific request.

13.2 You acknowledge that you will not obtain ownership rights in any information relating to and derived from Card transactions. Cardholder account numbers, personal information and other Card transaction information, including any databases containing such information, may not be sold or disclosed to a third party as an asset upon a bankruptcy, insolvency or failure of Client's business. Upon a bankruptcy, insolvency or failure of Client's business all Card transaction information must be returned to Servicers or acceptable proof of the destruction of all Card transaction information must be provided to Servicers.

14 **Assignments**

14.1 Any transfer or assignment of this Agreement by you, without our prior written consent, by operation of law or otherwise, is voidable by us. Furthermore, you shall indemnify and hold us harmless from all liabilities, Chargebacks, expenses, costs, fees and fines arising from such transferee's or assignee's Submission of Card transactions to us for processing. For purposes of this Section 14, any transfer of voting control shall be considered an assignment or transfer of this Agreement.

14.2 The payment Services provided by us require access to a single bank account in which we may initiate both Credits and debits. You may not enter into any agreement that would require, in any circumstance or event, the transfer of any payments or proceeds from Credit Card transactions covered by this Agreement to the custody or control of any third party. You may not assign any rights, including the right of payment under this Agreement, to any other person. In the event that you make an assignment (or provide a security interest) of receivables covered by this Agreement, then we may, at our option, elect to: (a) refuse to acknowledge such assignment unless accompanied by an Authorization to both initiate debits or Credits to the bank account of the assignee, (b) terminate this Agreement immediately, or (c) charge for any transfers that we are called upon to make manually to fulfill such an assignment at the rate of $100 per transfer.

14.3 Upon notice to you, another Visa and MasterCard member may be substituted for Bank under whose sponsorship this Agreement is performed with respect to Visa and MasterCard transactions. Upon substitution, such other Visa and MasterCard member shall be responsible for all obligations required of Bank for Visa and MasterCard transactions, including without limitation, full responsibility for its bank Card program and such other obligations as may be expressly required by applicable Association Rules.

14.4 Subject to Association Rules, we may assign or transfer this Agreement and our rights and obligations hereunder and/or may delegate our duties hereunder, in whole or in part, to any third party, whether in connection with a change in sponsorship, as set forth in the preceding sentence, or otherwise, without notice to you or your consent.

14.5 Except as set forth elsewhere in this Section and as provided in the following sentence, this Agreement shall be binding upon successors and assigns and shall inure to the benefit of the parties and their respective permitted successors and assigns. No assignee for the benefit of creditors, custodian, receiver, trustee in bankruptcy, debtor in possession, or other person charged with taking custody of a party's assets or business, shall have any right to continue, assume or assign this Agreement.

15 **Term; Account Closure Fee**

15.1 This Agreement shall become effective upon the date this Agreement is approved by our Credit Department.

15.2 The initial term of this Agreement shall be for one (1) month ("Initial Term") and shall continue in force on a month to month basis until either party terminates the Agreement upon written notice to the other.

15.3 Notwithstanding the above or any other provisions of this Agreement, we may terminate this Agreement at any time and for any reason by providing 30 days' advance notice to you. We may terminate this Agreement immediately or with shorter notice upon an Event of Default as provided under Section 17 of this Agreement. In the event we provide notice to you of an increase in the fees for Services, pursuant to Section 10.5, you may terminate this Agreement without further cause or penalty by providing us 30 days advance written notice of termination. You must terminate within 30 days after we provide notice of the Section 10.5 fee increase. The Section 10.5 fee increase shall not take effect in the event you provide timely notice of termination. However, your continued use of our Services after the effective date of any increase shall be deemed acceptance of the increased fees for Services, throughout the term of this Agreement.

15.4 **INTENTIONALLY OMITTED.**

16 **Amendments.** Subject to Section 15, we may amend this Merchant Agreement at any time by providing written notice to you of any amendment at least 20 days prior to the effective date of the amendment.

17 **Events of Default.** If any of the following events shall occur (each an "Event of Default") we may immediately terminate this Merchant Agreement without notice (a) a material adverse change in your business, financial condition, business procedures, prospects, products or services; (b) any assignment or transfer of voting control of you or your parent; or (c) a sale of all or a substantial portion of your assets; or (d) irregular Card sales by you, excessive Chargebacks, noncompliance with any applicable data security standards, as determined by Servicers, of any Card Association, or any other entity, or an actual or suspected data security breach, or any other circumstances which, in our sole discretion, may increase our exposure for your Chargebacks or otherwise present a financial or security risk to us; or e) any of your representations or warranties in this Agreement are breached in any material respect or are incorrect in any material respect when made or deemed to be made; or (f) you shall default in any material respect in the performance or observance of any term, covenant, condition or agreement contained in this Agreement, including, without limitation, the establishment or maintenance of funds in a Reserve Account, as detailed in Section 18; or (g) you shall default in any material respect in the performance or observance of any term, covenant or condition contained in any agreement with any of our affiliates; or (h) you shall default in the

payment when due, of any material indebtedness for borrowed money; or (i) you shall file a petition or have a petition filed by another party under the Bankruptcy Code or any other laws relating to bankruptcy, insolvency or similar arrangement for adjustment of debts; consent to or fail to contest in a timely and appropriate manner any petition filed against it in an involuntary case under such laws; apply for or consent to, or fail to contest in a timely and appropriate manner, the appointment of, or the taking of possession by, a receiver, custodian, trustee or liquidator of itself or of a substantial part of its property; or make a general assignment for the benefit of creditors; or take any corporate action for the purpose of authorizing any of the foregoing; or (j) your independent certified accountants shall refuse to deliver an unqualified opinion with respect to your annual financial statements and your consolidated subsidiaries; or (k) a violation by you of any applicable law or Association Rule or our reasonable belief that termination of this Agreement or suspension of Services is necessary to comply with any law including without limitation the rules and regulations promulgated by the Office of Foreign Assets Control of the US Department of the Treasury or your breach, as determined by Servicers, of Section 26.2 ("Compliance with Laws"); then, upon the occurrence of (1) an Event of Default specified in items (d), (i), or (k), we may consider this Agreement to be terminated immediately, without notice, and all amounts payable hereunder shall be immediately due and payable in full without demand or other notice of any kind, all of which are expressly waived by you, and (2) any other Event of Default, this Agreement may be terminated by us giving not less than 10 days' notice to you, and upon such notice all amounts payable hereunder shall be due and payable on demand.

17.1 Neither the expiration nor termination of this Agreement shall terminate the obligations and rights of the parties pursuant to provisions of this Agreement which by their terms are intended to survive or be perpetual or irrevocable. Such provisions shall survive the expiration or termination of this Agreement. All obligations by you to pay or reimburse us for any obligations associated with transactions you have submitted to us are intended to survive termination of this Agreement.

17.2 If any Event of Default shall have occurred and regardless of whether such Event of Default has been cured, we may, in our sole discretion, exercise all of our rights and remedies under applicable law, and this Agreement including, without limitation, exercising our rights under Section 18.

17.3 In the event you file for protection under the Bankruptcy Code or any other laws relating to bankruptcy, insolvency, assignment for the benefit of creditors or similar laws, and you continue to use our Services, it is your responsibility to open new accounts to distinguish pre-filing and post-filing obligations. You acknowledge that as long as you utilize the accounts you established prior to such filing, we will not be able to systematically segregate your post-filing transactions or prevent set-off of the pre-existing obligations. In that event, you (or your bankruptcy trustee) will be responsible for submitting an accounting supporting any adjustments that you may claim.

17.4 The Associations often maintain lists of merchants who have had their Merchant Agreements or Card Acceptance rights terminated for cause. If this Agreement is terminated for cause, you acknowledge that we may be required to report your business name and the names and other information regarding its principals to the Associations for inclusion on such list(s). You expressly agree and consent to such reporting if you are terminated as a result of the occurrence of an Event of Default or for any reason specified as cause by Visa, MasterCard or Discover Network. Furthermore, you agree to waive and hold us harmless from and against any and all claims which you may have as a result of such reporting.

17.5 After termination of this Agreement for any reason whatsoever, you shall continue to bear total responsibility for all Chargebacks, fees, Credits and adjustments resulting from Card transactions processed pursuant to this Agreement and all other amounts then due or which thereafter may become due under this Agreement.

18 Reserve Account; Security Interest

18.1 You expressly authorize us to establish a Reserve Account pursuant to the terms and conditions set forth in this Section 18. The amount of such Reserve Account shall be set by us, in our sole discretion, based upon your processing history and the potential risk of loss to us as we may determine from time to time.

18.2 The Reserve Account shall be fully funded upon three (3) days' notice to you, or in instances of fraud or suspected fraud or an Event of Default, Reserve Account funding may be immediate. Such Reserve Account may be funded by all or any combination of the following: (i) one or more debits to your Settlement Account or any other accounts held by Bank or any of its affiliates, at any financial institution vested in the name of Client, any of its principals, or any of its guarantors, or if any of same are authorized signers on such account; (ii) any payments otherwise due to you, including any amount due from TeleCheck; (iii) your delivery to us of a letter of credit; or (iv) if we so agree, your pledge to us of a freely transferable and negotiable certificate of deposit. Any such letter of credit or certificate of deposit shall be issued or established by a financial institution acceptable to us and shall be in a form satisfactory to us. In the event of termination or expiration of this Agreement by any party, an immediate Reserve Account may be established without notice in the manner provided above. Any Reserve Account will be held by us for the greater of ten (10) months after termination or expiration of this Agreement or for such longer period of time as is consistent with our liability for Card transactions and Chargebacks in accordance with Association Rules. Your funds will be held in an account commingled with reserve funds of our other Clients, without involvement by an independent escrow agent. Unless specifically agreed in writing by us or specifically required by applicable law, funds held by us in a Reserve Account shall not accrue interest. Notwithstanding the foregoing, we shall be entitled to accrued interest on any such funds held.

18.3 If your funds in the Reserve Account are not sufficient to cover the Chargebacks, adjustments, fees and other charges due from you, or if the funds in the Reserve Account have been released, you agree to promptly pay us such sums upon request.

18.3.1 To secure your obligations to Servicers and our affiliates under this Agreement and any other agreement for the provision of related equipment or related services (including any obligations for which payments on account of such obligations are subsequently invalidated, declared to be fraudulent or preferential, set aside or required to be repaid to a trustee, receiver or any other party under any bankruptcy act, state or federal law, common law or equitable cause), you grant to Servicers a first priority lien and security interest in and to (i) the Reserve Account; and (ii) any of your funds pertaining to the Card transactions contemplated by this Agreement now or hereafter in the possession of Servicers, whether now or hereafter due or to become due to you from Servicers. Any such funds, money or amounts now or hereafter in the possession of Servicers may be commingled with other funds of Servicers, or, in the case of any funds held pursuant to the foregoing paragraphs, with any other funds of other customers of Servicers. In addition to any rights now or hereafter granted under applicable law and not by way of limitation of any such rights, Servicers are hereby authorized by you at any time and from time to time, without notice or demand to you or to any other person (any such notice and demand being hereby expressly waived), to set off, recoup and to appropriate and to apply any and all such funds against and on account of your obligations to Servicers and their affiliates under this Agreement and any other agreement with Servicers or any of Servicers' affiliates for any related equipment or related services (including any check services), whether such obligations are liquidated, unliquidated, fixed, contingent, matured or unmatured. You agree to duly execute and deliver to Servicers such instruments and documents as Servicers may reasonably request to perfect and confirm the lien, security interest, right of set off, recoupment and subordination set forth in this Agreement.

18.3.2 To the extent funds are held in a separate Reserve Account, the Reserve Account shall be subject to (i) Servicers' security interest pursuant to this subsection 18.3.2; and (ii) an account control agreement (as defined by the applicable sections of the Uniform Commercial Code, hereinafter referred to as "Control Agreement") among you, the institution at which the Reserve Account is held (such institution hereinafter referred to as " Settlement Account") and Servicers (such investment account hereinafter referred to as the "Control Account"). The Control Agreement shall be in form and substance satisfactory to Servicers. The Settlement Account shall be a National Association bank which is mutually acceptable to you and Servicers.

18.3.3 For sake of clarification and notwithstanding anything in the Agreement to the contrary, in the event Servicers deduct, holdback, suspend, off set or set off (collectively "Set Off Funds") any settlement

monies or amounts otherwise due you pursuant to the terms of this Agreement, you acknowledge that such Set Off Funds will be held in a commingled Reserve Account (s) of Servicers (as described in this subsection 18.3.3) unless such Set Off Funds are wired or deposited by Servicers into any Control Account, pursuant to a Control Agreement in which case Servicers will transfer Set Off Funds from their commingled Reserve Account(s) to the Control Account as soon as practicable using commercially reasonable efforts.

18.3.4 If in replacement of or in addition to the first priority lien and security interest in the Reserve Account, you grant to Servicers a first priority lien and security interest in and to one or more certificates of deposit, the certificates of deposit shall be uncertificated and shall be subject to an Acknowledgement of Pledge of Certificate of Deposit and Control Agreement (the "Certificate of Deposit Control Agreement") by, between and among Customers, Servicers and the financial institution that has established and issued the certificate of deposit. The form of the Certificate of Deposit Control Agreement and the financial institution that will establish and issue the certificate of deposit shall be satisfactory and acceptable to Servicers.

19 Financial And Other Information

19.1 You will provide such other financial statements and other information concerning your business and your compliance with the terms and provisions of this Agreement as we may reasonably request. You authorize us to obtain from third parties financial and credit information relating to you in connection with our determination whether to accept this Agreement and our continuing evaluation of the financial and credit status of you. We may also access and use information which you have provided to Bank for any other reason related to provisioning of the Services. Upon request, you shall provide to us or our representatives reasonable access to your facilities and records for the purpose of performing any inspection and/or copying of your books and/or records deemed appropriate. In such event, you shall pay the costs incurred by us for such inspection, including, but not limited to, costs incurred for airfare and hotel accommodations.

19.2 You will provide us with written notice of any judgment, writ, warrant of attachment, execution or levy against any substantial part (25% or more in value) of your total assets not later than 3 days after you become aware of same.

20 Indemnification

20.1 You agree to indemnify and hold us harmless from and against all losses, liabilities, damages and expenses: (a) resulting from any breach of any warranty, covenant or agreement or any misrepresentation by you under this Agreement; (b) arising out of your or your employees' or your agents' negligence or willful misconduct, in connection with Card transactions or otherwise arising from your provision of goods and services to Cardholders; (c) arising out of your use of our Service; or (d) arising out of any third party indemnifications we are obligated to make as a result of your actions (including indemnification of any Association or Issuer).

20.2 We agree to indemnify and hold you harmless from and against all losses, liabilities, damages and expenses resulting from any breach of any warranty, covenant or agreement or any misrepresentation by us under this Agreement or arising out of our or our employees' gross negligence or willful misconduct in connection with this Agreement; provided that this indemnity obligation shall not apply to Bank with respect to Discover Network Card Transactions, American Express Card Transactions and Other Services, including JCB Card, PIN Debit Card, and Electronic Benefits Transfer Transactions, TeleCheck check services, TRS collection services, Gift Card Services, and Transactions involving Cards from other Non-Bank Card Associations such as Voyager Fleet Systems, Inc., Wright Express Corporation and Wright Express Financial Services Corporation.

21 Special Provisions Regarding Non-Bank Cards

21.1 Non-Bank Card transactions are provided to you by Processor and not by Bank. Bank is not a party to this Agreement insofar as it relates to Non-Bank Card services, and Bank is not liable to you in any way with respect to such services. For the purposes of this section, the words "we," "our," and "us" refer only to the Processor and not to the Bank. You authorize us to share information from your Application with American Express, JCB, or any other Non-Bank Card Association.

21.2 You understand that American Express transactions are processed, authorized and funded by American Express. American Express will provide you with its own agreement that governs those transactions. You understand and agree that we are not responsible and assume absolutely no liability with regard to any such transactions, including but not limited to the funding and settlement of American Express transactions, and that American Express will charge additional fees for the services they provide.

21.3 You understand that American Express is subject to separate approval—rates and fees as stated in your Merchant Application and Agreement are based on Client type and estimated volume and are subject to change. A Discount Rate will be collected by American Express. A $7.95 Monthly Fee is mandatory for all American Express mail order, telephone order, home-based and Internet physical delivery Clients for up to $5,000.00 in charge volume within any consecutive 12-month period and will be assessed by American Express. This monthly fee applies to online statements. Paper statements may be subject to additional fees. American Express pay frequency is three (3) days.

21.4 If you accept JCB Cards, you must securely retain original JCB Sales Drafts and JCB Credit Drafts for a period of at least 120 days from the date of the JCB Card transaction and you must retain microfilm or legible copies of JCB Sales Drafts and JCB Credit Drafts for a period of at least three (3) years following the date of the transaction.

21.5 If you accept JCB Cards you agree to be bound by JCB rules. You also agree to be bound by all other provisions of this Agreement which are applicable to JCB.

21.6 If you accept Voyager and/or WEX Cards, you agree to be bound by the WEX and/or Voyager rules. You also agree to be bound by all other provisions of this Agreement which are applicable to WEX and/or Voyager.

21.7 If you execute a WEX Merchant Agreement, you understand that we will provide such agreement to WEX, but that neither we nor WEX shall have any obligation whatsoever to you with respect to processing WEX Cards unless and until WEX executes your WEX Merchant Agreement. If WEX executes your WEX Merchant Agreement and you accept WEX Cards, you understand that WEX transactions are processed, authorized and funded by WEX. You understand that WEX is solely responsible for all agreements that govern WEX transactions and that we are not responsible and assume absolutely no liability with regard to any such agreements or WEX transactions, including but not limited to the funding and settlement of WEX transactions. You understand that WEX will charge additional fees for the services that it provides.

21.8 If you accept Voyager Cards:

- In addition to the information stated in Section 1 (MasterCard, Visa and Discover Network Acceptance) of the Operating Procedures, you should check Fleet Cards for any printed restrictions at the point of sale.
- In addition to the information provided under Section 1.5 (Special Terms) of the Operating Procedures, you shall establish a fair policy for the exchange and return of merchandise. You shall promptly submit credits to us for any returns that are to be credited to a Voyager Cardholder's account. Unless required by law, you shall not give any cash refunds to any Voyager Card holder in connection with a sale.
- In addition to the information required under Section 3.1 (Information Required) of the Operating Procedures, the following information must be contained on the single page document constituting the Sales Draft for Voyager transactions:
    - Time of transaction
    - Type of fuel sold
    - As permitted by the applicable POS device, odometer reading
    - For all cashier-assisted Sales Drafts and credit vouchers processed manually using a card Imprinter if required, the identification number
- If an increase in the number of Voyager transaction authorization calls from you not due to our or Voyager system outages in excess of 15% for a given month as compared to the previous month occurs, we may, in our discretion, deduct telephone charges, not to exceed $.25 (25 cents) per call, for the increased calls, from your settlement of your Voyager transactions.
- In addition to the information provided under Section 6 (Settlement) of the Operating Procedures, settlement of Voyager

transactions will generally occur by the fourth banking day after we process the applicable card transactions. We shall reimburse you for the dollar amount of sales submitted for a given day by you, reduced by the amount of Chargebacks, tax exemptions, discounts, credits, and the fees set forth in the Merchant Application. Neither we nor Voyager shall be required to reimburse you for sales submitted more than sixty (60) days from the date of purchase.

- For daily transmission of sales data, you shall maintain true and complete records in connection with the information required to be provided under this paragraph for a period of not less than thirty-six (36) months from the date of the generation of the data. You may store records on electronic media. You are responsible for the expense of retaining sales data records and Sales Drafts.
- In addition to the scenarios identified in Section 9.1.4 of the Operating Procedures that could cause an authorization related Chargeback to occur, with respect to Voyager transactions, Chargebacks shall be made in accordance with any other Voyager rules. Notwithstanding termination or expiration of this paragraph or the Agreement, you shall remain liable for all outstanding Chargebacks on Voyager transactions.
- In addition to the information provided under Section 12 (Representations; Warranties; Limitations of Liability; Exclusion of Consequential Damages), in no event shall our cumulative liability to you for losses, claims, suits, controversies, breaches or damages for any cause whatsoever in connection with Voyager transactions exceed the lesser of $10,000.00 or the Voyager transaction fees paid by you to us for the two months prior to the action giving arise to the claim.
- Notwithstanding anything in this Agreement to the contrary, our obligation to provide services to you relating to any Fleet Card will terminate automatically without penalty to us or the related Association upon the earlier of (i) the termination or expiration of our agreement with such Association, (ii) at least 20 days prior written notice by us to you, (iii) your failure to comply with material terms relating to such Fleet Card transactions, or (iv) written notice, if an Association discontinues its Card.

22 Special Provisions for PIN Debit Card

The special provisions outlined in this Section 22 apply only to those PIN Debit Card transactions that are processed by a Cardholder entering a PIN. These provisions do not apply to Non-PIN Debit Card transactions which do not involve entry of a PIN.

22.1 **PIN Debit Card Acceptance.** Most, but not all, ATM Cards (Debit Cards) can be accepted at the point of sale at participating locations. Examine the back of the PIN Debit Card to determine if the Card participates in a network that you are authorized to accept. Network mark(s) are usually printed on the back of the Card. If the PIN Debit Card is valid and issued by a participating network, you must comply with the following general requirements for all participating networks, in addition to the specific requirements of the network:

- You must honor all valid PIN Debit Cards when presented that bear authorized network marks.
- You must treat transactions by Cardholders from all Issuers in the same manner.
- You may not establish a minimum or maximum transaction amount for PIN Debit Card acceptance.
- You may not require additional information, besides the Personal Identification Number, for the completion of the transaction unless the circumstances appear suspicious. A signature is not required for PIN Debit Card transactions.
- You shall not disclose transaction related information to any party other than your agent, a network, or issuing institution and then only for the purpose of settlement or error resolution.
- You may not process a Credit Card transaction in order to provide a refund on a PIN Debit Card transaction.

22.2 **Transaction Processing.** The following general requirements apply to all PIN Debit Card transactions:

- All PIN debit transactions must be authorized and processed electronically. There is no Voice Authorization or Imprinter procedure for PIN Debit Card transactions.
- You may not complete a PIN Debit Card transaction that has not been authorized. If you cannot obtain an Authorization at the time of sale, you should request another form of payment from the customer or process the transaction as a Store and Forward or Resubmission, in which case you assume the risk that the transaction fails to authorize or otherwise declines. The Cardholder should be instructed to contact the Issuer to find out why a transaction has been declined.
- You may not complete a PIN Debit Card transaction without entry of the Personal Identification Number (PIN) by the Cardholder. The PIN must be entered into the PIN pad only by the Cardholder. You cannot accept the PIN from the Cardholder verbally or in written form.
- The PIN Debit Network used to process your transaction will depend upon, among other things, the availability of the network at the time of the transaction, whether a particular PIN Debit Card is enabled for a particular network and the routing requirements established by the networks and the card issuers. We may, at our sole discretion, utilize any PIN Debit Network available to us for a given transaction.
- You must issue a receipt to the Cardholder upon successful completion of a transaction. The Cardholder account number must be masked so that only the last four digits will appear. The masked digits must appear as a non-numeric character such as an asterisk. This is referred to as PAN truncation.
- You may not manually enter the account number. The account number must be read electronically from the Magnetic Stripe. If the Magnetic Stripe is unreadable, you must request another form of payment from the customer.
- Any applicable tax must be included in the total transaction amount for which Authorization is requested. Tax may not be collected separately in cash.
- YOU ARE RESPONSIBLE TO SECURE YOUR TERMINALS AND TO INSTITUTE APPROPRIATE CONTROLS TO PREVENT EMPLOYEES OR OTHERS FROM SUBMITTING REFUNDS AND VOIDS THAT DO NOT REFLECT BONA FIDE RETURNS OR REIMBURSEMENTS OF PRIOR TRANSACTIONS.

22.3 **Cash Back From Purchase.** You have the option of offering cash back to your customers when they make a PIN Debit Card purchase. You may set a minimum and maximum amount of cash back that you will allow. If you are not now offering this service, your terminal may require additional programming to begin offering cash back.

22.4 **Settlement.** Within one Business Day of the original transaction, you must balance each location to the system for each Business Day that each location is open.

22.5 **Adjustments.** An adjustment is a transaction that is initiated to correct a PIN Debit Card transaction that has been processed in error. You will be responsible for all applicable adjustment fees that may be charged by a Debit Card network. Some networks may have established minimum amounts for adjustments.

There are several reasons for adjustments being initiated:

- The Cardholder was charged an incorrect amount, either too little or too much.
- The Cardholder was charged more than once for the same transaction.
- A processing error may have occurred that caused the Cardholder to be charged even though the transaction did not complete normally at the point of sale.

All parties involved in processing adjustments are regulated by time frames that are specified in the operating rules of the applicable Debit Card network, The Electronic Funds Transfer Act, Regulation E, and other applicable law.

23 Special Provisions Regarding Electronic Benefit Transfer (EBT)

If you elect to engage in EBT transactions, the terms and conditions of this Section 23 shall apply.

EBT Transactions are provided to you by Processor and not by Bank. Bank is not a party to this Agreement insofar as it relates to EBT Transactions, and Bank is not liable to you in any way with respect to such services. For the purposes of this section, the words "we," "our," and "us" refer only to the Processor and not to the Bank. If you have agreed to issue Cash Benefits and will provide cash back or cash only transactions, you agree to maintain adequate cash on hand to issue confirmed Cash Benefits and will issue Cash Benefits to EBT customers in the same manner and to the same extent cash is provided to your other customers. You may not require that any EBT customers purchase goods or services as a condition to receiving

Cash Benefits, unless such condition applies to other customers as well. You may not designate special checkout lanes restricted to use by EBT customers unless you also designate special checkout lanes for debit or Credit Cards and/or other payment methods.

23.1 **Acceptance of EBT Benefits.** You agree to issue benefits to EBT customers in accordance with the procedures specified in all documentation provided to you by us, as amended from time-to-time and pursuant to all applicable law, rules and regulations. You must provide each EBT customer a receipt for each EBT transaction.

You will issue EBT benefits to EBT customers, in accordance with our then current procedures, in the amount authorized through a point-of-sale terminal, with personal identification number pad and printer. In the event of an equipment failure, you must comply with applicable procedures regarding manual voucher authorization. You must also comply with the procedures set forth in the Quest Operating Rules, as amended from time-to-time, issued by the National Automated Clearing House Association and approved by the Financial Management Service of the U.S. Treasury Department, and any additional rules, regulations and procedures specified by any additional state or federal government or agency regarding lost EBT Cards, forgotten PINs, discrepancies in benefits authorized and similar matters by referring EBT customers to their applicable EBT customer service center.

You may not accept any EBT Card for any purpose other than the acceptance of benefits, including without limitation acceptance of any EBT Card as security for repayment of any customer obligation. In the event of any violation of this provision, you will be obligated to reimburse the applicable state or us for any benefits unlawfully received. Cash should never be dispensed for Food Stamp Benefits.

23.2 **Manual EBT Vouchers.** All manual voucher authorizations must be cleared on your POS terminal for payment of voucher to be made to you. Vouchers must be cleared within 10 Business Days of voice authorization. Vouchers cannot be cleared by any manner except by your POS terminal therefore you should never mail vouchers requesting payment. If a voucher expires before it has been cleared by your POS for payment, no further action can be taken to obtain payment for the voucher. You must not attempt to voice authorize a manual EBT transaction if the EBT customer is not present to sign the voucher. A copy of the voucher should be given to the EBT customer at the time of authorization and you should retain one copy for your records.

23.3 **Acceptance of EBT Cash Benefits.** If you have agreed to issue Cash Benefits and will provide cash back or cash only transactions, you agree to comply with all applicable laws, rules and regulations and maintain adequate cash on hand to issue confirmed Cash Benefits and will issue Cash Benefits to EBT customers in the same manner and to the same extent cash is provided to your other customers. You may not require that any EBT customers purchase goods or services as a condition to receiving Cash Benefits, unless such condition applies to other customers as well. You may not designate special checkout lanes restricted to use by EBT customers unless you also designate special checkout lanes for debit or Credit Cards and/or other payment methods.

23.4 **Interoperability**. If you issue EBT benefits (Food Stamps and/or Cash Benefits), you must issue EBT benefits from EBT customers from all states.

23.5 **Required Licenses**. If you issue benefits under this Agreement, you represent and warrant to us that you are properly authorized to enter such transactions and are not currently disqualified or withdrawn from redeeming food stamp coupons or otherwise disqualified or withdrawn by any applicable agency. You agree to secure and maintain at your own expense all necessary licenses, permits, franchises, or other authorities required to lawfully effect the issuance and distribution of benefits under this Agreement, including without limitation, any applicable franchise tax certificate and non-governmental contractor's certificate, and covenant that you will not issue benefits at any time during which you are not in compliance with the requirements of any applicable law.

23.6 **Term and Termination.** If you are disqualified or withdrawn from the food stamp program, your authority to issue benefits will be terminated contemporaneously therewith. Such disqualification or withdrawal will be deemed a breach of this Agreement with respect to services or your relationship with that third party provider, and Servicers are in no way responsible for providing, maintaining, servicing or supporting such third party voice and/or data services.

24 **Purchase of Wireless Services.** In connection with your purchase of Wireless Equipment, you will purchase the Wireless Networks' service and obtain sublicenses to use any Wireless Software (as defined in Section 24.2) associated therewith (collectively "Wireless Services"). The prices that you will pay for the Wireless Services are set forth on the Schedule of Fees.

- Licenses. You agree to obtain any and all licenses, permits or other authorizations required by the Federal Communications Commission ("FCC") or any other regulatory authority, if any, for the lawful operation of Wireless Equipment used by you in connection with your receipt of Wireless Services. You will promptly provide us with all such information as we may reasonably request with respect to matters relating to the rules and regulations of the FCC.
- Improvements/General Administration. We and the Wireless Vendor(s) reserve the right to make changes, from time to time, in the configuration of the Wireless Services, Wireless Networks, Wireless Equipment, Wireless Software, rules of operation, accessibility periods, identification procedures, type and location of equipment, allocation and quantity of resources utilized, programming languages, administrative and operational algorithms and designation of the control center serving you at the particular address. In addition, we reserve the right to schedule, from time to time, interruptions of service for maintenance activities.

24.1 Software Licenses. We hereby grant to you a non-exclusive, non-transferable limited sublicense to use any Wireless Software solely in connection with your purchase and use of the Wireless Services. As used in this Section 24, "Wireless Software" means all software used in, for or in connection with the Wireless Equipment, the Wireless Services or the access thereto in whatever form, including without limitation source code, object code and microcode, including any computer programs and any documentation relating to or describing the Wireless Software. You acknowledge that the only right you obtain to the Wireless Software is the right to use the Wireless Software in accordance with the terms in this section.

24.2 Limitation on Liability. We shall have no liability for any warranties by any party with respect to uninterrupted Wireless Services, as set forth in Section 24.10, or for any third party's unauthorized access to Client's data transmitted through either the Wireless Equipment or Wireless Services, or Wireless Networks, regardless of the form of action (whether in contract, tort (including negligence), strict liability or otherwise). The foregoing notwithstanding, for any other liability arising out of or in any way connected with these Wireless Services terms, including liability resulting solely from loss or damage caused by partial or total failure, delay or nonperformance of the Wireless Services or relating to or arising from your use of or inability to use the Wireless Services, Processor's, Bank's, and Vendor(s)' liability shall be limited to your direct damages, if any, and, in any event, shall not exceed the amount paid by you for the particular Wireless Services during any period of failure, delay, or nonperformance of the Wireless Services. In no event shall Servicers, Wireless Vendor(s) or our respective affiliates be liable for any indirect incidental, special or consequential damages. The remedies available to you under these Wireless Services Terms will be your sole and exclusive remedies.

24.3 Indemnification. In addition to any other indemnifications as set forth in this Agreement, you will indemnify and hold Servicers, Vendor(s) and our respective officers, directors, employees, and affiliates harmless from and against any and all losses, claims, liabilities, damages, costs or expenses arising from or related to: (a) the purchase, delivery, acceptance, rejection, ownership, possession, use condition, liens against, or return of the Wireless Services; (b) your negligent acts or omissions; (c) any breach by you of any of your obligations under this Section 24; or (d) any third party's unauthorized access to Client's data and/or unauthorized financial activity occurring on your Merchant Account Number hereunder, except to the extent any losses, liabilities, damages or expenses result from our gross negligence or willful misconduct.

24.4 Confidentiality. All information or materials which could reasonably be considered confidential or competitively sensitive that you access from or relate to either Vendor(s) or Servicers related to the subject matter of these Wireless Services Terms will be considered confidential information. You will safeguard our confidential information

with at least the same degree of care and security that you use for your confidential information, but not less than reasonable care.

24.5 Termination. In addition to any other provision in this Agreement, the Wireless Services being provided under this Section 24 may terminate:

(a) Immediately upon termination of the agreement between us (or our affiliates) and Vendor(s), provided that we will notify you promptly upon our notice or knowledge of termination of such agreement, provided further that if Vendor(s) loses its authority to operate less than all of the Wireless Services or if the suspension of any authority or non-renewal of any license relates to less than all of the Wireless Services, then these Wireless Services Terms will terminate only as to the portion of the Wireless Services affected by such loss of authority, suspension or non-renewal; or

(b) Immediately if either we or our affiliates or Vendor(s) are prevented from providing the Wireless Services by any law, regulation, requirement, ruling or notice issued in any form whatsoever by judicial or governmental authority (including without limitation the FCC).

24.6 Effect of Termination. Upon termination of this Wireless Services Terms for any reason, you will immediately pay to us all fees due and owing to us hereunder. If these Wireless Services Terms terminate due to a termination of the agreement between us or our affiliates and Vendor(s), then we may, in our sole discretion, continue to provide the Wireless Services through Vendor(s) to you for a period of time to be determined as long as you continue to make timely payment of fees due under these Wireless Services Terms.

24.7 **Third Party Beneficiaries.** Our affiliates and Vendor(s) are third party beneficiaries of these Wireless Services Terms and may enforce its provisions as if a party hereto.

24.8 **Other Applicable Provisions.** You also agree to be bound by all other terms and conditions of this Agreement.

24.9 **Disclaimer.** Wireless Services use radio transmissions, so Wireless Services can't be provided unless your Wireless Equipment is in the range of one of the available Wireless Networks' transmission sites and there is sufficient network capacity available at that moment. There are places, particularly in remote areas, with no service at all. Weather, topography, buildings, your Wireless Equipment, and other conditions we don't control may also cause failed transmissions or other problems. PROCESSOR, BANK, AND VENDOR(S) DISCLAIM ALL REPRESENTATIONS AND WARRANTIES RELATING TO WIRELESS SERVICES. WE CANNOT PROMISE UNINTERRUPTED OR ERROR-FREE WIRELESS SERVICE AND DO NOT AUTHORIZE ANYONE TO MAKE ANY WARRANTIES ON OUR BEHALF.

24.10 **Special Provisions Regarding Wireless Service**

If you elect to purchase any Wireless Equipment from us as indicated on the Application, then the following terms and conditions of this Section 24, referred to as the Wireless Services Terms, shall apply. THE WIRELESS SERVICES ARE NOT BEING SOLD TO YOU FOR HOME OR PERSONAL USE. Sale of Wireless Services is made by Processor and not the Bank. Bank is not a party to this Agreement insofar as it relates to Wireless Services, and Bank is not liable to you in any way with respect to such services. For the purposes of this section, the words "we," "our," and "us" refer only to the Processor and not to the Bank.

Through our affiliates, we have acquired the right to resell and sublicense certain wireless POS Terminals and accessories (the "Wireless Equipment") and wireless data communication services using radio base stations and switching offered by the various cellular telephone and data networks throughout the country (the "Wireless Networks") in order to allow you to capture and transmit to us certain wireless Credit and Debit Card Authorization transactions or to transmit other communications to our system.

You acknowledge that one or more independent third party vendors ("Wireless Vendor(s)") has developed and provides the Wireless Equipment and Wireless Services to us through our affiliates under separate agreement(s).

In the event you elect to purchase voice and/or data services directly from a third party provider for use with the Wireless Equipment as permitted by Processor, you acknowledge and agree that the Agreement does not address or govern those voice and/or data.

24.11 **Waiver of Jury Trial.** ALL PARTIES IRREVOCABLY WAIVE ANY AND ALL RIGHTS THEY MAY HAVE TO A TRIAL BY JURY IN ANY JUDICIAL PROCEEDING INVOLVING ANY CLAIM RELATING TO OR ARISING UNDER THIS AGREEMENT.

25 **Other Terms**

25.1 **Force Majeure.** No party shall be liable for any default or delay in the performance of its obligations under this Agreement if and to the extent such default or delay is caused, directly or indirectly, by (i) fire, flood, earthquake, elements of nature or other acts of God; (ii) any terrorist attacks or outbreak or escalation of hostilities, war, riots or civil disorders in any country; (iii) any act or omission of the other party or any government authority; (iv) any labor disputes (whether or not employees' demands are reasonable or within the party's power to satisfy); or (v) the nonperformance by a third party for any similar cause beyond the reasonable control of such party, including without limitation, failures or fluctuations in telecommunications or other equipment. In any such event, the non-performing party shall be excused from any further performance and observance of the obligations so affected only for as long as such circumstances prevail and such party continues to use commercially reasonable efforts to recommence performance or observance as soon as practicable. Notwithstanding anything to the contrary in this paragraph, your failure to receive payment or funds from a third party shall not excuse the performance of your obligations to us under this Agreement.

25.2 Your authority to issue Cash Benefits and, in the event of such disqualification, we shall have the right to immediately terminate the provision of service under this Section 23.6 or the Agreement in its entirety. With respect to the issuance of Cash Benefits only, your authority to issue Cash Benefits may be suspended or terminated immediately at the sole discretion of us, the state or its EBT service provider, effective upon delivery of a notice of suspension or termination specifying the reasons for such suspension or termination if there shall be (i) any suspension, injunction, cessation, or termination of the EBT service provider's authority to provide EBT services to the state; (ii) failure by you, upon not less than thirty (30) days prior written notice, to cure any breach by you of the provisions of these terms and conditions, including without limitation, your failure to support the issuance of benefits during your normal business hours consistent with your normal business practices, your failure to comply with issuance procedures, impermissible acceptance of an EBT Card, or your disqualification or withdrawal from the food stamp program; or (iii) based on a state's or its EBT service provider's investigation of the relevant facts, evidence that you or any of your agents or employees are committing, participating in, or have knowledge of fraud or theft in connection with the dispensing of benefits. In the event you fail to cure any breach as set forth above, you may appeal such suspension of termination to the applicable state for determination in its sole discretion.

In the event that your authority to accept benefits is suspended or terminated by a state or its EBT service provider, and you successfully appeal such suspension or termination to the state or its EBT service provider, we shall be under no obligation to reinstate the services previously provided.

The provision of services under this Section 23.6 shall terminate automatically in the event that our Agreement or our service provider's agreement with any applicable state's EBT service provider terminates for any reason.

25.3 **Confidentiality of EBT System Information.** All information related to EBT recipients and/or the issuance of benefits shall be considered confidential information.

Individually identifiable information relating to a benefit recipient or applicant for benefits will be held confidential and will not be disclosed by you or your directors, officers, employees or agents, without prior written approval of the applicable state.

The use of information obtained by you in the performance of your duties under this Section 23.7 will be limited to purposes directly connected with such duties.

25.4 **EBT Service Marks.** You will adequately display any applicable state's service marks or other licensed marks, including the Quest mark, and other materials supplied by us (collectively the "Protected Marks") in accordance with the standards set by the applicable state. You will use the Protected Marks only to indicate that benefits are issued at your location(s) and will not indicate that we, any state or its EBT service provider or we endorses your goods or services. Your right to use such Protected Marks pursuant to this Agreement will continue only so long as this Agreement remains in effect or until you

are notified by us, any state or its EBT service provider to cease their use or display.

25.5 **Miscellaneous**

25.5.1 **Amendments.** If any of these terms and conditions are found to conflict with federal or state law, regulation or policy of the rules, these terms and conditions are subject to reasonable amendment by a state or its EBT service provider to address such conflict upon 20 days written notice to you provided that you may, upon written notice, terminate your obligation under this Section 23 upon receipt of notice of such amendment.

25.5.2 **State Action.** Nothing contained herein shall preclude a state from commencing appropriate administrative or legal action against you or for making any referral for such action to any appropriate federal, state, or local agency.

26 **Compliance with Laws.**

In performing its obligations under this Agreement, each party agrees to comply with all laws and regulations applicable to it. You further agree to cooperate and provide information requested by Servicers, as Servicers determine necessary, to facilitate Servicers compliance with any applicable law including without limitation the rules and regulations promulgated by the Office of Foreign Assets Control of the US Department of the Treasury.

26.1 Notices. Except as otherwise specifically provided, all notices and other communications required or permitted hereunder (other than those involving normal operational matters relating to the processing of Card transactions) shall be in writing, shall be sent by mail, courier or facsimile (facsimile notices shall be confirmed in writing by courier), if to you at your address appearing in the Application and if to us at P.O. Box 5180, Simi Valley, CA 93062, facsimile: 805-552-8899, with a copy to Attention: General Counsel's Office, 3975 N.W. 120th Avenue, Coral Springs, FL 33065, and shall be deemed to have been given (i) if sent by mail or courier, when mailed or delivered, and (ii) if sent by facsimile machine, when the courier confirmation copy is actually received. Notice given in any other manner shall be effective when actually received. Notices sent to the Merchant's last known address, as indicated in our records, shall constitute effective notice to the Merchant under this Agreement.

26.2 Headings. The headings contained in this Agreement are for convenience of reference only and shall not in any way affect the meaning or construction of any provision of this Agreement.

26.3 Severability. The parties intend every provision of this Agreement to be severable. If any part of this Agreement is not enforceable, the remaining provisions shall remain valid and enforceable.

26.4 Entire Agreement; Waiver. This Agreement constitutes the entire Agreement between the parties with respect to the subject matter thereof, and supersedes any previous agreements and understandings. A party's waiver of a breach of any term or condition of this Agreement shall not be deemed a waiver of any subsequent breach of the same or another term or condition.

26.5 Amendment. We may modify any provision of this Agreement by providing written notice to you. You may choose not to accept the requirements of any such change by terminating the Agreement within twenty (20) days of receiving notice. If you choose to do so, notify us that you are terminating for this reason so that we may waive any Early Cancellation Fee that might otherwise apply. For purposes of this section, an electronic or "click-wrap" notice intended to modify or amend this Agreement and which you check "I Accept" or "I Agree" or otherwise accept through an electronic process, shall constitute in writing as required herein.

26.6 No Third Party Beneficiaries. Nothing in this Agreement is intended to confer upon any person or entity other than the parties any rights or remedies, and the parties do not intend for any third parties to be third-party beneficiaries of this Agreement.

26.7 Association Rules. The parties acknowledge that the Visa, MasterCard and Discover Network Association Rules give Visa, MasterCard and Discover Network certain rights to require termination or modification of this Agreement with respect to transactions involving Visa, MasterCard and Discover Network Cards and the Visa, MasterCard and Discover Network Card systems and to investigate you. The parties also acknowledge that issuers of other Cards, for which we perform services on your behalf, may have similar rights under their applicable Association Rules with respect to this Agreement's applicability to transactions involving such other Cards.

26.8 Publicity. Client may not use our logo, name, trademark, or service mark in any manner, including without limitation, in any advertisements, displays, or press releases, without our prior written consent.

THIRD PARTY AGREEMENTS

The following Agreements are Third Party Agreements entered into between Client and the Third Parties identified in the Third Party Agreements.

If Client desires to receive the products and/ or services offered under a Third Party Agreement, Client must check the appropriate box or otherwise indicate such desire in the Merchant Application, in which case the terms and conditions of the Third Party Agreement shall be binding upon Client. The Signature page in the Merchant Application and Agreement shall also serve as a signature page to the Third Party Agreements.

Client acknowledges that the Third Parties are relying upon the information contained on the Merchant Application, all of which are incorporated by reference into the Third Party Agreements.

27 **EQUIPMENT LEASE AGREEMENT**

This Equipment Lease Agreement ("Lease Agreement") is being entered into by and between First Data Merchant Services Corporation (through its business unit First Data Global Leasing), and the Lessee identified on the signature panel of this Merchant Processing Application ("MPA"). In this Lease Agreement, the words "we", "our" and "us" refer to First Data Merchant Services Corporation and its successors and assigns and the words "you" and "your" refer to Lessee and its permitted successors and assigns.

Lessee hereby authorizes us or our designees, successors or assigns (hereinafter "Lessor") to withdraw any amounts including any and all sales taxes now due or hereinafter imposed, owed by Lessee in conjunction with this Lease Agreement by initiating debit entries to the bank account designated by Lessee on the MPA (the "Settlement Account"). In the event of default of Lessee's obligation hereunder, Lessee authorizes debit of its account for the full amount due under this Lease Agreement. Further, Lessee authorizes its financial institution to accept and to charge any debit entries initiated by Lessor to Lessee's account. In the event that Lessor withdraws funds erroneously from Lessee's account, Lessee authorizes Lessor to credit Lessee's account for an amount not to exceed the original amount of the debit. This authorization is to remain in full force and effect until Lessor has received written notice from Lessee of its termination in such time and in such manner as to afford Lessor a reasonable opportunity to act. Lessee also authorizes Lessor from time to time to obtain investigative credit reports from a credit bureau or a credit agency concerning Lessee.

27.1 Equipment. We agree to lease to you and you agree to lease from us the equipment identified on the MPA or such other comparable equipment we provide you (the "Equipment"), according to the terms and conditions of this Lease Agreement. We are providing the Equipment to you "as is" and make no representations or warranties of any kind as to the suitability of the Equipment for any particular purpose. The term Equipment includes the Equipment initially deployed under the Lease Agreement and/or any additions, replacements, substitutions, or additions thereto.

27.2 Effective Date, Term and Interim Rent.

(a) This Lease Agreement becomes effective on the earlier of the date we deliver any piece of Equipment to you (the "Delivery Date") or acceptance by us. This Lease Agreement remains in effect until all of your obligations and all of our obligations under it have been satisfied. We will deliver the Equipment to the site designated by you.

(b) The term of this Lease Agreement begins on a date designated by us after receipt of all required documentation and acceptance by us (the "Commencement Date"), and continues for the number of months indicated on the MPA. THIS IS A NON-CANCELABLE LEASE FOR THE TERM INDICATED.

(c) You agree to pay an Interim Lease Payment in the amount of one-thirtieth ($1/30^{th}$) of the monthly lease charge for each day from and including the Delivery Date until the date preceding the Commencement Date.

(d) YOU ACKNOWLEDGE THAT THE EQUIPMENT AND/OR SOFTWARE YOU LEASE UNDER THIS LEASE AGREEMENT MAY NOT BE COMPATIBLE WITH ANOTHER PROCESSOR'S SYSTEMS AND THAT WE DO NOT HAVE ANY OBLIGATION TO MAKE SUCH SOFTWARE AND/OR EQUIPMENT COMPATIBLE IN THE EVENT THAT YOU ELECT TO USE ANOTHER SERVICE PROVIDER. UPON TERMINATION OF YOUR MERCHANT PROCESSING AGREEMENT, YOU ACKNOWLEDGE THAT YOU MAY NOT BE ABLE TO USE THE EQUIPMENT AND/OR SOFTWARE LEASED UNDER THIS LEASE AGREEMENT WITH SAID SERVICE PROVIDER.

27.3 Site Preparation. You will prepare the installation site(s) for the Equipment, including but not limited to the power supply circuits and phone lines, in conformance with the manufacturer's and our specifications and will make the site(s) available to us by the confirmed shipping date.

27.4 Payment of Amounts Due.

(a) The monthly lease charge is due and payable monthly, in advance. You agree to pay all assessed costs for delivery and installation of Equipment.

(b) In addition to the monthly lease charge, you shall pay, or reimburse us for, amounts equal to any taxes, assessments on or arising out of this Lease Agreement or the Equipment, and related supplies or any services, use or activities hereunder, including without limitation, state and local sales, use, property, privilege and excise tax, tax preparation, compliance expenses, but exclusive of taxes based on our net income. Property taxes are calculated and charged based on the average of the estimated annual property taxes over the course of the term of the lease. You will also be charged an annual Tax Handling Fee, as set forth in the MPA and/or applicable Fee Schedule.

(c) Your lease payments will be due despite dissatisfaction with the Equipment for any reason.

(d) Whenever any payment is not made by you in full when due, you shall pay us as a late charge, an amount equal to ten percent of the amount due but no less than $5.00 for each month during which it remains unpaid (prorated for any partial month), but in no event more than the maximum amount permitted by law. You shall also pay to us an administrative charge of $10.00 for any debit we attempt to make against your Settlement Account that is rejected.

(e) In the event your account is placed into collections for past due lease amounts, you agree that we can recover a collection expense charge of $50.00 for each aggregate payment requiring a collection effort.

27.5 Use and Return of Equipment; Insurance.

(a) You shall cause the Equipment to be operated by competent and qualified personnel in accordance with any operating instructions furnished by us or the manufacturer. You shall maintain the Equipment in good operating condition and protect it from deterioration, normal wear and tear excepted.

(b) You shall not permit any physical alteration or modification of the Equipment, or change the installation site of the Equipment, without our prior written consent.

(c) You shall not create, incur, assume or allow to exist any consensually or judicially imposed liens or encumbrances on, or part with possession of, or sublease the Equipment without our prior written consent.

(d) You shall comply with all governmental laws, rules and regulations relating to the use of the Equipment. You are also responsible for obtaining all permits required to operate the Equipment at your facility.

(e) We or our representatives may, at any time, enter your premises for purposes of inspecting, examining or repairing the Equipment.

(f) The Equipment shall remain our personal property and shall not under any circumstances be considered to be a fixture affixed to your real estate. You shall permit us to affix suitable labels or stencils to the Equipment evidencing our ownership.

(g) You shall keep the Equipment adequately insured against loss by fire, theft, and all other hazards.

(h) You shall provide proof of insurance. The loss, destruction, theft or damage of or to the Equipment shall not relieve you from your obligation to pay the full purchase price or total monthly lease charges hereunder.

27.6 Title to Equipment. The Equipment is, and shall at all times be and remain, our sole and exclusive property, and you shall have no right, title or interest in or to the Equipment except as expressly set forth in this Lease Agreement or otherwise agreed in writing. Except as expressly provided in Section 28.8, no transference of intellectual property rights is intended by or conferred in this Lease Agreement. You agree to execute and deliver to us any statement or instrument that we may request to confirm or evidence our ownership of the Equipment, and you irrevocably appoint us as your attorney-in-fact to execute and file the same in your name and on your behalf. If a court determines that the leasing transaction contemplated by this Lease Agreement does not constitute a financing and is not a lease of the Equipment, then we shall be deemed to have a first lien security interest on the Equipment as of the date of this Lease Agreement, and you will execute such documentation as we may request to evidence such security interest. If this Lease Agreement is deemed a loan despite the intention of the parties, then in no contingency or event whatsoever shall interest deemed charged hereunder, however such interest may be characterized or computed, exceed the highest rate permissible under any law which a court of competent jurisdiction shall, in a final determination, deem applicable hereto.

27.7 Return or Purchase of Equipment at End of Lease Period. Upon the completion of your lease term or any extension, you will have the option to; (a) return the Equipment to us, or (b) purchase the Equipment from us for the lesser of fair market value at the time (as determined in good faith by us) or an amount equal to ten-percent (10%) of the total lease payments under this Lease Agreement with respect to each item of Equipment. In the absence of an affirmative election by you to return or purchase the Equipment, this lease will continue on a month-to-month basis at the existing monthly lease payment; or (c) after the final lease payment has been received by FDGL, the Agreement will revert to a month by month rental at the existing monthly lease payment. If Client does not want to continue to rent the equipment, then Client will be obligated to provide FDGL with 30 day prior written notice to terminate and return the equipment to FDGL. If we terminate this Lease Agreement pursuant to Section 28.12 (b) due to a default by you, then you shall immediately return the Equipment to us no later than the tenth Business Day after termination, or remit to us the fair market value of the Equipment as determined in good faith by us. We may collect any amounts due to us under this Section 28.7 by debiting your Settlement Account, and to the extent we are unable to obtain full satisfaction in this manner, you agree to pay the amounts owed to us promptly upon our request.

27.8 Software License. We retain all ownership and copyright interest in and to all computer software, related documentation, technology, know-how and processes embodied in or provided in connection with the Equipment other than those owned or licensed by the manufacturer of the Equipment (collectively "Software"), and you shall have only a nonexclusive license to use the Software in your operation of the Equipment.

27.9 Limitation on Liability. We are not liable for any loss, damage or expense of any kind or nature caused directly or indirectly by the Equipment, including any damage or injury to persons or property caused by the Equipment. We are not liable for the use or maintenance of the Equipment, its failure to operate, any repairs or service to it, or by any interruption of service or loss of use of the Equipment or resulting loss of business. Our liability arising out of or in any way connected with this Lease Agreement shall not exceed the aggregate lease amount paid to us for the particular Equipment involved. In no event shall we be liable for any indirect, incidental, special or consequential damages. The remedies available to you under this Lease Agreement are your sole and exclusive remedies.

27.10 Warranties.

(a) All warranties, express or implied, made to you or any other person are hereby disclaimed, including without limitation, any warranties regarding quality, suitability, merchantability, fitness for a particular purpose, quiet enjoyment, or non-infringement.

(b) You warrant that you will only use the Equipment for commercial purposes and will not use the Equipment for any household or personal purposes.

27.11 Indemnification. You shall indemnify and hold us harmless from and against any and all losses, liabilities, damages and expenses resulting from (a) the operation, use, condition, liens against, or return of the Equipment or (b) any breach by you of any of your obligations

hereunder, except to the extent any losses, liabilities, damages or expenses result from our gross negligence or willful misconduct.

27.12 Default; Remedies.

(a) If any debit of your Settlement Account initiated by us is rejected when due, or if you otherwise fail to pay us any amounts due hereunder when due, or if you default in any material respect in the performance or observance of any obligation or provision of this Lease Agreement or any agreement with any of our affiliates or joint ventures, any such event shall be a default hereunder. Without limiting the foregoing, any default by you under a processing agreement with us or with an affiliate or joint venture to which we are a party will be treated as a default under this Lease Agreement. Such a default would include a default resulting from early termination of the MPA.

(b) Upon the occurrence of any default, we may at our option, effective immediately without notice, either (i) terminate this lease and our future obligations under this Lease Agreement, repossess the Equipment and proceed in any lawful manner against you for collection of all charges that have accrued and are due and payable, or (ii) accelerate and declare immediately due and payable all monthly lease charges for the remainder of the applicable lease period together with the fair market value of the Equipment (as determined by us), not as a penalty but as liquidated damages for our loss of the bargain. Upon any such termination for default, we may proceed in any lawful manner to obtain satisfaction of the amounts owed to us and, if applicable, our recovery of the Equipment, including entering onto your premises to recover the Equipment. In any case, you shall also be responsible for our costs of collection, court costs, as well as applicable shipping, repair and refurbishing costs of recovered Equipment. You agree that we shall be entitled to recover any amounts due to us under this Lease Agreement by charging your Settlement Account or any other funds of yours that come into our possession or control, or within the possession or control of our affiliates or joint ventures, or by setting off amounts that you owe to us against any amounts we may owe to you, in any case without notifying you prior to doing so. Without limiting the foregoing, you agree that we are entitled to recover amounts owed to us under this Lease Agreement by obtaining directly from an affiliate or joint venture to which we are a party and with which you have entered into an MPA any funds held or available as security for payment under the terms of the MPA, including funds available under the "Reserve Account; Security Interest" section of the MPA, if applicable.

27.13 Assignment. You may not assign or transfer this Lease Agreement, by operation of law or otherwise, without our prior written consent. For purposes of this Lease Agreement, any transfer of voting control of you or your parent shall be considered an assignment or transfer of this Lease Agreement. We may assign or transfer this Lease Agreement and our rights and obligations hereunder, in whole or in part, to any third party without the necessity of obtaining your consent.

27.14 Lease Guaranty. No guarantor shall have any right of subrogation to any of our rights in the Equipment or this Lease Agreement or against you, and any such right of subrogation is hereby waived and released. All indebtedness that exists now or arises after the execution of this Lease Agreement between you and any guarantor is hereby subordinated to all of your present and future obligations, and those of your guarantor, to us, and no payment shall be made or accepted on such indebtedness due to you from a guarantor until the obligations due to us are paid and satisfied in full.

27.15 Governing Law; Venue; Miscellaneous. This Lease Agreement shall be governed by and will be construed in accordance with the laws of the State of New York (without applying its conflicts of laws principles). The exclusive venue for any actions or claims arising under or related to this Lease Agreement shall be in the appropriate state of federal court located in Suffolk County, New York. If any part of this Lease Agreement is not enforceable, the remaining provisions will remain valid and enforceable.

27.16 Notices. All notices must be in writing, and shall be given (a) if sent by mail, when received, and (b) if sent by courier, when delivered; if to you at the address appearing on the MPA, and if to us at 4000 Coral Ridge Drive, Coral Springs, Florida 33065. Attn: Lease Department. Customer Service toll free number 1-877-257-2094.

27.17 Entire Agreement. This Lease Agreement constitutes the entire Agreement between the parties with respect to the Equipment, supersedes any previous agreements and understandings and can be changed only by a written agreement signed by all parties. This Lease Agreement may be executed in any number of counterparts and all such counterparts taken together shall be deemed to constitute one and the same instrument. Delivery of an executed counterpart of a signature page of this Lease Agreement by facsimile shall be effective as delivery of a manually executed counterpart of this Lease Agreement.

Glossary

As used in this Agreement, the following terms mean as follows:

Acquirer: Banks in the case of MasterCard, Visa and certain debit transactions or network acquirers in the case of Discover Network transactions that acquire Card sale transactions from merchants such as yourself.

Address Verification: A service provided through which the merchant verifies the Cardholder's address, in whole or in part. Primarily used by Mail/Telephone/Internet order merchants, Address verification is intended to deter fraudulent transactions. However, it is not a guarantee that a transaction is valid.

Agreement: The Agreements among Client, Processor and Bank, contained in the Application, the Program Guide and the Schedules thereto and documents incorporated therein, each as amended from time to time, which collectively constitute the Agreement among the parties.

Application: See Merchant Application.

Association: Any entity formed to administer and promote Cards, including without limitation MasterCard International, Incorporated ("MasterCard"), Visa U.S.A., Inc. and Visa International ("Visa"), DFS Services, LLC ("Discover Network") and any applicable debit networks.

Association Rules: The rules, regulations, releases, interpretations and other requirements (whether contractual or otherwise) imposed or adopted by any Association.

Authorization: Approval by, or on behalf of, the Card Issuer to validate a transaction for a merchant or another affiliate bank. An Authorization indicates only the availability of the Cardholder's Credit Limit at the time the Authorization is requested.

Authorization Approval Code: A number issued to a participating merchant by the Authorization Center which confirms the Authorization for a sale or service.

Authorization Center: A department that electronically communicates a merchant's request for Authorization on Credit Card transactions to the Cardholder's bank and transmits such Authorization to the merchant via electronic equipment or by voice Authorization.

Authorization Fee: A Client is charged an Authorization Fee each time communication is made with the host (other than when a Merchant transmits a batch for settlement, for which the Client is charged a Batch Closure Fee) via the POS terminal, software or gateway.

Bank: The bank identified on the Application signed by you.

Bankruptcy Code: Title 11 of the United States Code, as amended from time to time.

Batch: A single Submission to us of a group of transactions (sales and Credits) for settlement. A Batch usually represents a day's worth of transactions.

Business Day: A day (other than Saturday or Sunday) on which Bank is open for business.

Card: See either Credit Card or Debit Card.

Card Issuer: The bank or Association that issues a Card to an individual.

Card Validation Codes: A three-digit value printed in the signature panel of most Cards and a four-digit value printed on the front of an American Express Card. Visa's Card Validation Code is known as CVV2; MasterCard's Card Validation Code is known as CVC2; Discover Network's Card Validation Code is known as a CID. Card Validation Codes are used to deter fraudulent use of an account number in a non-face-to-face environment, (e.g. mail orders, telephone orders and Internet orders).

Card Verification Value (CVV)/Card Validation Code (CVC): A unique value encoded on the Magnetic Stripe of a Card used to validate Card information during the Authorization process.

Card Not Present Sale/Transaction: A transaction that occurs when the Card is not present at the point-of-sale, including Internet, mail-order and telephone-order Card sales.

Cardholder: The individual whose name is embossed on a Card (or Debit Card, as applicable) and any authorized user of such Card.

Cash Benefits: An EBT account maintained by an Issuer that represents pre-funded or day-of-draw benefits, or both, administered by one or more Government entities, and for which the Issuer has agreed to provide access under the EBT program. Multiple benefits may be combined in a single cash benefit account.

Cash Over Transaction: Dispensing of cash by a merchant in connection with a Card sale, other than a PIN Debit Card transaction, for the purchase of goods or services.

Chargeback: The procedure by which a Sales Draft or other indicia of a Card transaction (or disputed portion) is returned to Bank, the Acquirer or the Issuer. Client is responsible for reimbursing us for all Chargebacks.

Chargeback Fee: A fee incurred each time a transaction is charged back to you

Client: The party identified as "Client" on the Application. The words "Subscriber," "you" and "your" refer to Client.

Compliance Svc Fee: For Clients in good standing, payment of the Compliance Fee will cover the costs of one PCI questionnaire per year, or if an Internet scan is required, four scans per year for one IP address from a data security vendor approved by Processor, while Client has an open account with Processor. If Client has more than one IP address that requires scanning, Client is responsible for any such scans. These benefits are subject to change without notice. The payment of the Compliance Svc Fee does not affect your compliance responsibilities and obligations associated with your Merchant Account.

Credit: A refund or price adjustment given for a previous purchase transaction.

Credit Card: A valid Card authorizing the Cardholder to buy goods or services on credit and bearing the service mark of Visa, MasterCard or Discover Network and, to the extent the Schedules so provide, a valid Card authorizing the Cardholder to buy goods or services on credit and issued by any other Association specified on such Schedules.

Credit Card Operating Procedures: The manual prepared by Processor, containing operational procedures, instructions and other directives relating to Card transactions.

Credit Draft: A document evidencing the return of merchandise by a Cardholder to a Client, or other refund made by the Client to the Cardholder.

Credit Limit: The credit line set by the Card Issuer for the Cardholder's account.

Customer Activated Terminal (CAT): A magnetic stripe terminal or chip-reading device (such as an automatic dispensing machine, Limited Amount Terminal, or Self-Service Terminal) that is not an ATM.

Debit Card: See either PIN Debit Card or Non-PIN Debit Card.

Debit Network Processing Fees: Fees charged by PIN Debit networks for processing PIN Debit Transactions. In addition to any Debit Network Processing Fees, Client will also pay the Debit Card/ATM transaction fee as indicated in the Merchant Application and Agreement. Debit Network Processing Fees are subject to change without notice.

Dial-Up Terminal: An Authorization device which, like a telephone, dials an Authorization Center for validation of transactions.

Discount Rate: An amount charged a merchant for processing its qualifying daily Credit Card transactions. Transactions that fail to meet applicable interchange requirements will be charged additional amounts as set forth in Section 10.1 and the "Discount Rates for MasterCard/Visa/Discover Network" section of the Merchant Application and Agreement.

Early Cancellation Fee: A fee in an amount equal to $300.00, charged in the event that: a) you elect to cancel this Merchant Agreement prior to the expiration of the initial term of the Merchant Agreement; or b) the Merchant Agreement is terminated prior to the expiration of the initial term due to an Event of Default, except as provided in Section 15.3.

Electronic Benefit Transfer (EBT): An electronic system that allows a government benefit recipient to authorize the transfer of their benefits from a Federal, State or local government account to a merchant account to pay for products and services received.

Electronic Draft Capture (EDC): A process which allows a merchant's Dial-Up Terminal to receive Authorization and capture transactions, and electronically transmit them to a Card Processor. This eliminates the need to submit paper for processing.

Factoring: The submission of authorization requests and/or Sales Drafts by a merchant for Card sales or Cash Advances transacted by another business.

Gross: When referred to in connection with transaction amounts or fees, refers to the total amount of Card sales, without set-off for any refunds or Credits.

Imprinter: A manual or electric machine used to physically imprint the merchant's name and ID number as well as the Cardholder's name and Card number on Sales Drafts.

Issuer: The bank or Association which has issued a Card to an individual. MasterCard and Visa only issue Cards through banks ("Issuing Banks") while Discover Network may issue Cards directly or issue Cards through an issuing bank.

Limited Amount Terminal: A Customer Activated Terminal that has data capture only capability, and accepts payment for items such as parking garage fees, road tolls, motion picture theater entrance, or magnetic-stripe telephones.

Magnetic Stripe: A stripe of magnetic information affixed to the back of a plastic Credit or Debit Card. The Magnetic Stripe contains essential Cardholder and account information.

Media: The documentation of monetary transactions (i.e., Sales Drafts, Credit Drafts, computer printouts, etc.).

Merchant Identification Card: A plastic embossed Card supplied to each merchant to be used for imprinting information to be submitted with each Batch of paper Sales Drafts. Embossed data includes Merchant Account Number, name and sometimes merchant ID code and terminal number.

Merchant Account Number (Merchant Number): A number that numerically identifies each merchant, outlet, or line of business to the Processor for accounting and billing purposes.

Merchant Agreement: The agreement among Client, Processor, TWI PPS and Bank contained in the Merchant Application and Agreement, any attachments, addenda, schedules thereto, each as amended from time to time, all of which collectively constitute the agreement among the parties. Bank is a party to this Merchant Agreement for Visa MasterCard and non-PIN debit purposes only.

Merchant Application: The Application portion of the Merchant Application and Agreement sometimes referred to as the "Application".

Monthly Account Fee: A recurring monthly fee, as indicated in your Merchant Application and Agreement, for maintaining an account with Processor.

Monthly Customer Service Fee: A recurring monthly fee, as indicated in your Merchant Application and Agreement, for customer service access.

Monthly Minimum Fee: A fee, as indicated in the Merchant Application and Agreement, less the net Discount Rates, if any, for your applicable transactions during the month.

Non-PIN Debit Card: A Debit Card with either a Visa, MasterCard or Discover Network mark that is tied to a Cardholder's bank account or a prepaid account and which is processed without the use of a PIN.

Non-Qualified Interchange Fee: The difference between the interchange fee associated with the Anticipated Interchange Level and the interchange fee associated with the more costly interchange level at which the transaction actually processed.

Non Receipt of PCI Data Validation Fee: Fee charged on a monthly basis on accounts that have not confirmed their compliance or who have been deemed non-compliant.

Operating Procedures: The then-current manual prepared by Processor, containing operating procedures, instructions and other directives relating to Card transactions. If you process Card transactions, you must comply with the Operating Procedures. The current Operating Procedures are available online at http://www.paypros.com/fdmsdocs/ppiopguide0408.pdf.

Other Services: Other Services include all services related to , JCB Card, PIN Debit Card, and Electronic Benefits Transfer Transactions, TeleCheck check services, TRS collection services, Gift Card Services, and Transactions involving Cards from other Non-Bank Card Associations such as Voyager Fleet Systems, Inc., Wright Express Corporation and Wright Express Financial Services Corporation.

PAN Truncation: A procedure by which a Cardholder's copy of a Sales or Credit Draft will only reflect the last four digits of the Card account number.

PIN: A Personal Identification Number entered by the Cardholder to submit a PIN Debit Card transaction.

PIN Debit Card: A Debit Card used at a merchant location by means of a Cardholder-entered PIN in the merchant PIN Pad. PIN Debit Cards bear the marks of ATM networks (such as NYCE, Star).

PIN Debit Sponsor Banks: The PIN Debit Sponsor Bank(s) identified on the Application signed by you that is/are the sponsoring or acquiring bank(s) for certain PIN Debit networks.

Point of Sale (POS) Terminal: A device placed in a merchant location which is connected to the Processor's system via telephone lines and is designed to authorize, record and transmit settlement data by electronic means for all sales transactions with Processor.

Processor: The entity identified on this Application (other than the Bank) which provides certain services under this Agreement.

Recurring Payment Indicator: A value used to identify transactions for which a consumer provides permission to a merchant to bill the consumer's Card account at either a predetermined interval or as agreed by the Cardholder for recurring goods or services.

Referral: This message received from an Issuer when an attempt for Authorization requires a call to the Voice Authorization Center or Voice Response Unit (VRU).

Reserve Account: A fund established and managed by us to protect against actual or contingent liability arising from Chargebacks, adjustments, fees and other charges due to or incurred by us.

Resubmission: A transaction that the merchant originally processed as a Store and Forward transaction but received a soft denial from the respective debit network or Association. The resubmission transaction allows the merchant to attempt to obtain an approval for the soft denial, in which case you assume the risk that the transaction fails.

Retrieval Request/Transaction Documentation Request: A request for documentation related to a Card transaction such as a copy of a Sales Draft or other transaction source documents.

Sales Draft: Evidence of a purchase of goods or services by a Cardholder from Client using a Card, regardless of whether the form of such evidence is in paper or electronic form or otherwise, and may include a service order receipt), all of which must conform to Association Rules and applicable law.

Sales/Credit Summary: The identifying form used by a paper Submission merchant to indicate a Batch of Sales Drafts and Credit Drafts (usually one day's work). Not a Batch header, which is used by electronic merchants.

Schedules: The attachments, addenda and other documents, including revisions thereto, which may be incorporated into and made part of this Agreement.

Self-Service Terminal: A Customer Activated Terminal that accepts payment of goods or services such as prepaid cards or video rental, has electronic capability, and does not accept PINs.

Servicers: For Visa and MasterCard Credit and non-PIN debit Card transactions, Bank, Processor, TWI Payment Processing Services., collectively. For all other Card transactions, Processor. The words "us" and "we" refer to Servicers.

Services: The activities undertaken by Processor and Bank to authorize, process and settle all United States Dollar denominated Visa and MasterCard transactions undertaken by Cardholders at Client's location(s) in the United States, and all other activities necessary for Processor to perform the functions required by this Agreement for Discover Network and all other Cards covered by this Agreement.

Settlement Account: An account at a financial institution designated by Client as the account to be debited and credited by Processor or Bank for Card transactions, fees, Chargebacks and other amounts due under the Agreement or in connection with the Agreement.

Split Dial: A process which allows the Authorization terminal to dial directly to different Card processors (e.g., American Express) for Authorization. In this instance, the merchant cannot be both EDC and Split Dial. Split Dial is also utilized for Check Guarantee companies.

Split Dial/Capture: Process which allows the Authorization terminal to dial directly to different Card processors (e.g., Amex) for Authorization and Electronic Draft Capture.

Store and Forward: A transaction that has been authorized by a merchant when the merchant cannot obtain an Authorization while the customer is present, typically due to a communications failure. The merchant will store the transaction electronically in their host system and retransmit the transaction when communications have been restored.

Submission: The process of sending Batch deposits to Processor for processing. This may be done electronically or by mail.

Summary Adjustment: An adjustment to your Submission and/or Settlement Accounts in order to correct errors.

Telecommunication Card Sale: Individual local or long-distance telephone calls, for which the telephone service provider is paid directly by use of a Card. These do not include, however, calls paid for with pre-paid telephone service cards. Telecommunication Card Sales are considered Card Not Present Sales.

Third Party Agreement(s): If applicable, the agreements with third parties located in the Merchant Application and Agreement. These Third Party Agreements are separate and distinct from the Merchant Agreement with Processor and Bank and are subject to separate approvals.

Transaction Fees: Service costs charged to a merchant on a per transaction basis.

Us, We: See Servicers.

You, Your: See Client.

Appendix B City of Columbia's Cloud Computing Requirements

Responsibilities of the Cloud Vendors

All external cloud vendors, defined as vendors providing any cloud services as defined in this strategy to the City of Columbia must adhere to the following policies.

3.1 Records Requests

3.1.1 The vendor will respond to records request within the timeframe required by the City.

3.2 Using City of Columbia Domain Names

3.2.1 All cloud deployments that are intended to perform a service for our customers will be deployed using the gocolumbiamo.com domain name.

3.2.2 The City of Columbia IT Department will be the sole entity responsible for the gocolumbiamo.com domain name. The cloud vendor shall not expect to maintain DNS records belonging to the City of Columbia

3.2.2.1 The cloud vendor will provide the IP addresses used for the service prior to deployment. The City of Columbia IT Department will update the gocolumbiamo.com domain records accordingly.

3.2.2.2 The cloud vendor shall not change the addresses used with a frequency of greater than once per year

3.2.2.3 The cloud vendor shall notify the City of Columbia IT department in writing on official letterhead 30 days in advance of any IP address changes

3.2.2.4 The cloud vendor will use the gocolumbiamo.com only for the business purposes authorized by this agreement

3.2.3 Email from gocolumbiamo.com

When sending email from the service using the gocolumbiamo.com domain name, the following additional policies will be in effect

3.2.3.1 The cloud vendor will provide the IP addresses from which email will be sent. The City of Columbia IT Department will use this information to update the gocolumbiamo.com SPF record.

3.2.3.2 The addresses provided to the City of Columbia as required in 3.2.3.1 shall be only those IP addresses that are used to send email using the gocolumbiamo.com domain name.

3.2.3.3 The City of Columbia will update the gocolumbiamo.com SPF records according to the same policies and timelines as defined in 3.2.2 of this policy.

3.2.3.4 The cloud vendor will take all reasonable precautions to ensure that SPAM is not sent using the gocolumbiamo.com domain or from any IP address under cloud vendor control that has been associated with the gocolumbiamo.com domain.

3.2.3.5 The cloud vendor will react to email abuse reports in a timely manner

3.3 Standards and Regulations

3.3.1 The cloud vendor will adhere to relevant standards. For example, SaaS vendors deploying products over the web shall adhere to OWASP or similar standards.

3.3.2 The cloud vendor shall take responsibility for all regulatory compliance.

3.3.3 The cloud vendor shall conduct regular security audits of their systems. The security audits shall include internal and external review of system security and the security of all code used by the vendor. The vendor shall react promptly to mitigate the vulnerabilities identified by security audits.

3.4 System Integration

When an external cloud deployment requires access to existing information system infrastructure the following policies must be followed

3.4.1 Software should run with least possible privilege. For example, if database access needs to be given, the system account should have the least possible privilege; it should not run as a user that has access to schema outside of its need.

3.4.2 System account names should not be easily guessed. Passwords for these accounts should not be easily guessed and should be different from other customers with the same product. Connections from system accounts should be, where appropriate and possible, controlled via access lists.

3.5 Deployment and Customization

3.5.1 The cloud vendor shall disclose any authentication information that exists by default. The cloud vendor shall work with the City of Columbia to remove or change these accounts from their default values. The vendor shall not deploy services to the City of Columbia where system accounts are shared with other entities.

3.6 Encryption

3.6.1 Cloud vendor shall establish a suitable data encryption scheme for data in transit between the City of Columbia, its customers, and the vendor. The City of Columbia will determine the suitability of the encryption scheme.

3.6.2 Cloud vendor shall establish a suitable encryption for City of Columbia data while in storage for both live and backup media. The City of Columbia will determine the suitability of the encryption scheme.

3.6.3 No encryption scheme will be considered suitable if City of Columbia data can be recovered using the same decryption key as that of another customer of the cloud vendor.

3.7 Incident Preparation

3.7.1 The cloud vendor will take responsibility for keeping their system software up to date. Vendors should monitor relevant discussion boards and mailing lists for security problems with products they use.

3.7.2 The cloud vendors shall have a method for customers and others to report security problems. This method should be well publicized and accessible. Vendors should have a method for prioritizing and acting on reports of security problems.

3.7.3 The cloud vendors shall have a method for correcting discovered vulnerabilities. Vulnerabilities should be prioritized and corrected based on the risk vulnerability exploitation would pose to its customers. Vulnerability mitigation efforts should be tested by the vendor, as appropriate, prior to their release.

3.8 Incident Response

3.8.1 The cloud vendor will take responsibility for security incident handling if their system is compromised.

3.8.2 The cloud vendor shall immediately notify the City of Columbia of any breaches and will advise what information has been compromised. If this information is later found to be inaccurate the cloud vendor will immediately notify the City of Columbia with the correct information.

3.8.3 If investigation, containment, and eradication efforts by the City of Columbia incur costs while fault lies with the cloud vendor, the cloud vendor will assume the costs.

3.8.4 The cloud vendor will provide a rapid contact method for reporting suspected abuse, 24x7x365. The cloud vendor will react in a timely manner to abuse reports from the City of Columbia

3.8.5 The cloud vendor will provide their incident response plans. Response plans will include procedures for both security incident and disaster incident response.

SUMMATION360™
a TWI Innovation

TWI Product and Services Support Policy

This document provides TWI's maintenance and support policies for its products and services. It describes the scope of TWI support and the service levels provided.

SCOPE OF SUPPORT	On-Site Software / Hardware	Hosted Services
Installation	√	√
Configuration	√	√
Usability Issues (Citizen/Staff)	√	√
Problem Diagnosis / Resolution	√	√
Proactive System Notices	√	√
Software Updates[1]	√	√
Software Bug Fixes, Patches[2]	√	√
Hardware Repair and Replacement[3]	√	√
Virus Protection Policies, Procedures, Results		√
Security Policies, Procedures, Results		√
System/Network Design & Performance		√
Database API Support and Resolution		√
Telco Equipment/Provider Design & Performance		√
SERVICE LEVEL	**On-Site Software / Hardware**	**Hosted Services**
Number of Cases	Unlimited	Unlimited
Case Escalation Procedures	- As Necessary or - By Request	- As Necessary or - By Request
Non-Urgent Cases[5]		
-Hours of Coverage	Normal Business Hours[4]	Normal Business Hours[4]
-Support Channels	Email & Phone	Email & Phone
-Initial Response Time	1 Hour	1 Hour
-Ongoing Response Time	As Required Until Resolved	As Required Until Resolved
Urgent Cases[6]		
-Hours of Coverage	24/7/365	24/7/365
-Support Channels	Phone Only	Phone Only
-Initial Response Time (normal business hours / non-business hours)	1 hr / 2 hrs	1 hr / 2 hrs
-Ongoing Response Time	Daily Until Resolved	Daily Until Resolved

NOTES

1 – Software Updates: TWI will provide to Customer periodic updates and modifications to Licensed Software as and if they become generally available to correct functional deficiencies and incorporate minor new features and improvements.

2 – Software Bug Fixes, Patches: TWI shall use commercially reasonable efforts to promptly repair, correct or replace the Licensed Software in order to fix a design defect, after reasonable notice of same from Customer.

3 – Hardware Repair and Replacement: TWI will replace defective components of Hardware within a reasonable time of notice of a defect.

4 – Normal Business Hours: Defined as non-federal government holidays, Monday-Friday, 8:00am-7:00pm EST

5 – Non-Urgent Cases: TWI will provide product and technical support services during normal business hours. TWI shall respond by telephone and/or email within one (1) hour to any product issue reported during normal business hours to confirm receipt of the reported failure. Thereafter, TWI shall assign an appropriate internal resource to investigate, diagnose, provide status updates and resolve the reported problem for the Customer as necessary. (by email- customercare@ summation360.com and by phone- (540) 953-2631, option #3)

6 – Urgent Cases: TWI will provide product and technical support services 24 hours a day, 7 days a week, and 365 days a year.

- During normal business hours, TWI shall respond by telephone and/or email within one (1) hour to confirm receipt of the reported failure. Thereafter, TWI shall assign an appropriate internal resource to investigate, diagnose, and provide daily status updates and resolve the reported problem for the Customer. (by email- customercare@summation360.com and by phone- (540) 953-2631, option #3)
- Outside of normal business hours, TWI shall respond within two (2) hours to any product issue reported by telephone and marked "urgent" through the TWI's voice mail system. (by phone only- (540) 953-2631, option #3)

CONTACT TWI CUSTOMER CARE

Non-Urgent Issues	Urgent Issues
Normal Business Hours: (phone and email) (540) 953-2631 #3 customercare@summation360.com	Normal Business Hours: (phone and email) (540) 953-2631 #3 customercare@summation360.com Non-Business Hours: **(Phone Only)** (540) 953-2631 #3 – Leave a Voice Mail Marked "URGENT"

Red Flag Rule

City of Columbia Identity Theft Prevention Program

Effective December, 2010

City Council Adopted and Effective Date: _____

This document is intended to give guidance to the City in their understanding of the FTC Red Flag Rule. It is not intended to be used in place of compliance, in whole or any part, of the FTC Rule.
08/02/10 Final
11/10/10 Reviewed/Updated

D

Table of Contents

INTRODUCTION

The City of Columbia (the "City") has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003, pursuant to 16 C.F.R. §681.2. This Program is designed to detect, prevent and mitigate identity theft not only in connection with the opening and maintenance of City utility accounts but other city accounts, applications, registrations or other transactions, referred to as "Record" or "Records" throughout this Program, where identity theft might occur.

Why did FTC make this rule?
The intent is to protect consumers from identity theft. It is targeted at entities that **obtain** and **hold** consumer identification such as billing addresses, Social Security Numbers, dates of birth, passports or immigration documents, or other information.

Who must comply?
Entities such as Columbia that obtain and hold identification often targeted by identity thieves must comply.

What is a "Red Flag?"
A "Red Flag" is a term the FTC has coined to identify possible identity theft. It is a pattern or particular specific activity that indicates the possible risk of identity theft. The FTC has identified thirty-one "Red Flags" that entities, especially utilities, should watch for. Such entities are required to have a written plan to help employees identify these "Red Flags" and how to respond when a possible identity theft has occurred.

How does Columbia have to comply with this rule?
We have a duty to:

1. Identity Red Flags
2. Detect Red Flags; and
3. Respond to Red Flags

Who within City operations has to comply with the rule?
All City Departments which obtain and hold any of the consumer identification mentioned above must comply with the rule.

For purposes of this Program, "Identity Theft" is considered to be "fraud committed using the identifying information of another person." The Program "Record" is defined as:

1. A continuing relationship the City has with an individual through a Record the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account, registration, application or record the City offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the City from Identify Theft

This Program was developed with oversight and approval of the Columbia City Council. After consideration of the size and complexity of the City's operations and various systems, and the nature and scope of these activities, the Columbia City Council determined that this Program was appropriate for the City and therefore approved this Program on December 15, 2008.

The Red Flag Rule-City of Columbia Identity Theft Prevention Program was reviewed and amended December, 2010.

IDENTIFICATION OF RED FLAGS

A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. In order to identify relevant Red Flags, the City of Columbia considered risk factors such as the types of Records it offers and maintains, the methods it provides to open or establish these Records, the methods it provides to access its Records, and its previous experiences with Identity Theft. The City identified the following Red Flags in each of the listed Categories:

1. **Notifications and Warnings from Consumer Reporting Agencies**

    1) A fraud or activity alert that is included with a consumer report;

    2) Receiving a report or notice from a consumer reporting agency of a credit freeze;

    3) Receiving a report of fraud with a consumer report; and

    4) Receiving indication from a consumer report of activity that is inconsistent with a customer's usual pattern or activity.

2. **Suspicious Documents (see below) used in such a way (items 1-13)**

    - Lease
    - Death certificate
    - Driver's license
    - Immigration Papers or Work Card
    - Passport
    - Birth certificate
    - Student Identifications
    - Government Issued Identification
    - Military Identification
    - Non-Driver's License Identification
    - Credit and Debit Cards

    1) Receiving documents that are provided for identification that appear to be forged or altered;

    2) Receiving documentation on which a person's photograph or physical description is not consistent with the person presenting the documentation;

    3) Receiving other information on the identification not consistent with information provided by the person opening a new Record or customer presenting the identification;

4) Receiving other documentation with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged);

5) Receiving an application for service that appears to have been altered, forged or gives the appearance of having been destroyed and reassembled;

6) Personal identifying information provided is inconsistent when compared against external information sources used by the Department (such as the address does not match any address in the Consumer Report or the Social Security Number has not been issued, or is listed on the Social Security Death's Master File);

7) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal knowledge and/or external third party sources (telephone number or address on an application is the same as the telephone number or address provided on a fraudulent application;

8) Receiving verbal, written, or internet based information where the same person with the same billing information requests utility service at more than one location;

9) The Social Security Number provided is the same as that submitted by other person(s) opening a Record;

10) The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening Records;

11) The person opening a Record fails to provide all required personal identifying information (incomplete application);

12) The person opening a Record cannot provide authenticating information if requested to do so;

13) The Department is notified by a customer (s) with information that another customer may have opened a fraudulent Record.

3. Suspicious Personal Identifying Information

1) A person's identifying information is inconsistent with other sources of information (such as an address not matching an address on a Consumer Report or a Social Security Number that was never issued);

2) A person's identifying information is inconsistent with other information the customer provides (such as inconsistent Social Security Numbers, billing addresses or birth dates);

3) A person's identifying information is the same as shown on other applications found to be fraudulent;

4) A person's identifying information is consistent with fraudulent activity (such as an invalid phone number or a fictitious billing address);

5) A person's Social Security Number is the same as another customer's Social Security Number;

6) A person's address or phone number is the same as that of another person;

7) A person fails to provide complete personal identifying information on an application when reminded to do so; and

8) A person's identifying information is not consistent with the information that is on file for the customer.

9) The physical appearance of a customer does not match with other sources of information (such as driver's license, passport or immigration work card).

10) A person does not know the last 4 digits of his/her Social Security Number.

11) A new customer requests new service and a routine Social Security Number check locates an account with delinquent or a collection balance that is proved not to be the responsibility of the customer requesting new service.

4. Unusual Use Of or Suspicious Activity Related to a Record

1) A change of address for a Record followed by a request to change the Record holder's name or add other parties;

2) A new Record used in a manner consistent with fraud (such as the customer failing to make the first payment, or making the initial payment and no other payments);

3) A Record being used in a way that is not consistent with prior use (such as late or no payments when the Record has been timely in the past);

4) Mail sent to the Record holder is repeatedly returned as undeliverable;

5) The Department receives notice that a customer is not receiving his paper statements; and

6) The Department receives notice that a Record has unauthorized activity.

7) A Record is designated for shut-off due to non-payment and the customer at the location does not match the customer on file.

8) Unauthorized access to or use of customer records information such as log on or authentication failures.

5. Notice Regarding Possible Identity Theft

The City receives notice from a customer, an identity theft victim, law enforcement or any other person that it has opened or is maintaining a fraudulent Account for a person engaged in Identity Theft.

DETECTION OF RED FLAGS.

1. **In order to detect any of the Red Flags identified above with the opening of a new Record, City personnel will take the following steps and verify the identity of the person opening the Record:**

    1) Requiring certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, Social Security Number, driver's license or other identification;

    2) Verifying the customer's identity in person, such as by copying and reviewing a driver's license or other identification card;

    3) Reviewing documentation showing the existence of a business entity (in person process);

    4) Independently contacting the customer; and

    5) Requesting the customer to appear in person with appropriate information or documentation.

2. **In order to detect any of the Red Flags identified above for an existing Record, City personnel will take the following steps to monitor transactions with such information:**

    1) Verifying the identification of customers if they request information (in person, via telephone, via facsimile, via email);

    2) Verifying the validity of requests to change billing addresses;

    3) Verifying changes in banking information given for billing and payment purposes; and

    4) Verifying the last 4 digits of his/her Social Security Number.

PREVENTING AND MITIGATING IDENTITY THEFT

1. **In the event City personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:**

   1) Continuing to monitor a Record for evidence of Identity Theft;

   2) Person who may be or is suspected to be the possible victim of identity theft;

   3) Changing any passwords or other security devices that permit access to Records;

   4) Reopening a Record with a new number;

   5) Not opening a new Record;

   6) Closing an existing Record;

   7) Notifying law enforcement; See **Appendix D.**

      Example: If the City receives notice that its system has been compromised such that a customer's personal information has become accessible, at a minimum the City will notify the customer and change passwords.

      Example: If the City receives notice that a person has provided inaccurate identification information, the Record will be closed immediately and notify Law Enforcement.

   8) Determining that no response is warranted under the particular circumstances; or

      Example: If the City notices late payments on a Record regularly paid and determines the resident has been incapacitated, no action may be necessary.

   9) Notifying the Program Administrator for determination of the appropriate step (s) to take.

2. **In order to further prevent the likelihood of identity theft occurring with respect to Records the City will take the following steps with respect to its internal operating procedures:**

   1) Providing a secure website or clear notice that a website is not secure;

2) Ensuring complete and secure destruction of paper documents and computer files containing customer information. Paper documents and computer files containing customer information should be retained for the minimum retention required by law, unless there is a significant business purpose to retain the record for a longer period of time.

3) Requiring certain provisions included in city contracts with vendors. If the storage or destruction of paper documents and computer files are contracted to a private vendor, contracts must include a provision that requires the private vendor to store the documents and files in a secure manner so as to be accessible only by approved city personnel. Upon appropriate authorization by an approved city official, the vendor shall destroy the documents and computer files in a secure fashion. The storage and destruction of paper documents and computer files which contain sensitive information must be performed by either a city employee or a private vendor under contract.

4) Ensuring that office computers are password protected and that computer screens lock after a set period of time;

5) Requiring only the last 4 digits of Social Security Numbers on customer Records;

6) Requiring each Department review, no less than once a year, employee's access to Record information to determine if the employee's duties require such access and if the employee is complying with the provisions of the City Identity Theft Prevention Program. The Department shall restrict access as much as feasible and maintain an up to date list of those employees required to have access along with the date access was last reviewed. If the employee's access involves computer files, access shall be documented in the City Security Tracking System.

7) Prohibiting Record information to be written on sticky pads or note pads;

8) Ensuring that computer screens are only visible to the employee accessing the Record;

9) Requiring customers to authenticate addresses and personal information, rather than account representatives asking if the information is correct;

10) Maintaining secure office location;

11) Maintaining cameras in timely and good working order and providing for property destruction of tapes and other recording media;

12) Periodically (each Department) reviewing and maintaining a complete, accurate, and current internal list of authorized personnel and procedures with respect to the appropriate responses should a red flag occur or should the Department be aware of actual identity theft. Each Department with

access to such records shall provide periodic reports to the Red Flag Committee and Program Administrator. The report shall include red flags they have detected, their response, and any recommendations for changes in their Department internal policies and procedures and the City Identity Theft Prevention Program.

13) Should vendors have access to personal identifying information, Departments shall also include in contracts with vendors provisions for either the reporting of red flags to the Department or to require the vendor to prevent and mitigate the crime themselves. If the contract provides for the vendor to prevent and mitigate, the contract should also include a provision for periodic reports about the Red Flags the vendor detected and their response.

14) Each city department involved in the opening of new Records or maintenance of existing Records: Utility Customer Services, Parks and Recreation, and Information Systems shall maintain a complete, accurate, and current internal list of authorized personnel with respect to the appropriate responses in the event of a Red Flag occurring, having occurred or an actual Identity Theft; and

14) Because the City cannot predict all particular circumstances that may arise, City Personnel are requested to be diligent while not compromising customer service in the detection of other possible Red Flags.

UPDATING THE PROGRAM AND THE RED FLAGS

1) This Program will be reviewed and updated annually, or as needed, to reflect changes in risks to customers and the soundness of City Records from Identity Theft. An Assistant City Manager will be designated the Program Administrator and work with the **Red Flag Committee,** an internal City working group to consider the City's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of Records, and changes in the City's business arrangements with other entities. To do so, the Red Flag Committee and Program Administrator shall evaluate the effectiveness of the City Identity Theft Prevention Program, effectiveness of the monitoring of the practices of service providers, and will analyze significant incidents of identity theft and city response.

2) After considering these factors and recommendations from the Committee, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will present the Program and recommended changes to the City Council who will make a determination of whether to accept, modify or reject those changes to the Program.

3) **Note: Each City Department included in the Program shall conduct an annual Needs Assessment to ensure that their operation is current in identifying Red Flags and response protocol. See Appendix F.**

PROGRAM ADMINISTRATION AND TRAINING

1. Oversight.

The City's Program will be overseen by an Assistant City Manager and the Red Flag Committee. Committee members shall consist of the representatives of the City Manager's Office, and all other city Departments that obtain and hold personal identifying information. The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances, reviewing and, if necessary, approving changes to the Program.

2. Staff Training and Reports.

City staff responsible for implementing the Program shall be trained under the direction of the Program Administrator, the appropriate Department Head, the Police Department and/or a combination of the above in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. **See Appendix E.** Such training will be sufficient to effectively implement the Program. All training shall be conducted annually and documented. Vendors are required to either report any red flags to the Program Administrator or respond appropriately to prevent and mitigate the crime themselves.

3. Service Provider Arrangements.

The City will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1) Requiring, by contract, that service providers have such policies and procedures in place;

2) Requiring, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator; and,

3) Each Department is required to maintain an up-to-date written internal policy as it pertains to their internal security and identity theft.

Patricia Bollmann, Manager
City of Columbia, Utilities and Billing
PO Box 1676
Columbia MO 65205-1676
Phone 573-874-7458
Fax 573-874-7763
E-Mail PAB@gocolumbiamo.com

Appendix A

Finance Department Internal Identity Theft Policy
Utility Customer Services
Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Ordinance

POLICY: Any person or agency requesting information regarding a customer's account must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

Customers must identify themselves by the last 4 digits of their SS# before any information may be given on their account. If they can not give the last 4 digits of their SS# no information can be given.

- Telephone requests from the public for phone or social security numbers are always declined
- Persons requesting any information of a personal nature must come in person with picture ID and speak to the Manager/Supervisor.
- Faxed requests for personal information are not acceptable.
- For Realtors or prospective tenants/new homeowners it is acceptable to give information regarding high and low or average utility bills. It is not acceptable to disseminate any personal information in the notes, master file, or payment history.
- Requests for billing information from the file should only be given to the spouse, the significant other, or roommates listed in the master file or notes after they have provided the correct Social Security as verification.
- Governmental agencies; police or prosecutors requesting information should properly identify themselves. These calls should be handled by the Manager or Supervisor or the Collection staff.
- Any discussion of the details of customer's accounts outside of the office is never acceptable for any reason.
- When there is a confidential flag on an account, follow the instructions on the notes

Customer information on master file is password protected.

- Customers are not allowed in CSR Area
- Customer payment agreements are kept in the secure area.
- No paper documents may be left on desks

Janice W. Finley, Business Services Administrator
City of Columbia, Business License Division
PO Box 6015
Columbia MO 65205
Phone: 573-874-7747
Fax: 573-874-7761
E-Mail: Janice@GoColumbiaMo.com

Appendix A (cont'd)

Finance Department Internal Identity Theft Policy
Business License Division
Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Code-4 of Ordinances

POLICY: Any person or agency requesting information regarding a business license customer's confidential information in their license file must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

Identification of Red Flags

- Mail sent to the license applicant is repeatedly returned as undeliverable.
- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the license applicant.
- Receiving information from American DataBank Inc., the company that provides criminal background check services, concerning the inconsistency of a social security number and date of birth of a license applicant.
- The license applicant fails to provide the required personal identifying information (incomplete application).
- Receiving verbal or written information concerning an applicant submitting fraudulent documents.
- Applicant's driver's license photo is inconsistent with the person presenting the documentation.

- Owner of company listed on license application inconsistent with the Missouri Secretary of State records.

Detection of Red Flags

- Require identifying information from all license applicants.
- Verify the applicant's identity in person.
- Review documentation showing the existence of a business entity.
- Verify the identity of applicants, if they request information.

Preventing and Mitigating Identity Theft

- American Databank, Inc. monitors identifying information for inconsistencies in social security number, name, date of birth, and relays this information to the Business License Office.
- The invoices received from American Databank include only the last four digits of the applicants' social security number.
- Applicants' social security number and business gross receipts information are always deleted/blacked out on documents requested from a licensee's file.
- Social security and gross receipts information are never released unless requested by the applicant in person upon providing identification.
- Requests for confidential licensing information from City Police Department staff, Law Department staff, representatives from governmental agencies, etc., are required to obtain this information from the Business Services Administrator after providing identification.
- Inactive business license files are stored in a locked area.
- All Business License staff computers are password protected.
- Computer screens are only visible to the Business License employee when accessing licensing records.
- File cabinets that contain business license records, as well as hotel/motel and cigarette tax records, are locked at the end of each business day. The Business License area is never left unattended during office hours and access to this area is restricted to Business License staff and management.

- Always obtain copy of applicant's driver's license or other picture ID when applying for a license or permit.
- Check immigration papers to ensure validity.
- If an applicant fails to provide the requested personal identifying information, the license or permit application is denied.
- The appearance of altered or forged documents prompts further investigation.
- Double check with Missouri Secretary of State's Office to confirm members of a corporation are consistent with those listed on the application.
- Obtain criminal background check from previous state in which the applicant resided if the applicant has lived in Missouri for less than one year.
- Computer screen darkens or fades out when staff is away from their desks.
- The Business Services Administrator is the only person who can grant access to the business license system.

Ron Barrett, Comptroller
City of Columbia, Accounting Division
PO Box 6015
Columbia MO 65205
Phone: 573-874-7371
Fax: 573-874-7686
E-Mail: Ron@GoColumbiaMo.com

Appendix A (cont'd)

Finance Department Internal Identity Theft Policy
Miscellaneous Receivables Accounting Division
Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Code of Ordinances

POLICY: Any person or agency requesting information regarding a miscellaneous receivables customer's confidential information in their miscellaneous receivables file must have a demonstrated right to know

PROCEDURE:

Identification of Red Flags

- Mail sent to the miscellaneous receivable customer is repeatedly returned as undeliverable.
- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the miscellaneous receivable customer.
- Receiving verbal or written information concerning a miscellaneous receivable customer submitting fraudulent documents.
- Owner of company listed on miscellaneous receivable customer inconsistent with the MO Secretary of State records.

Detection of Red Flags

- Review documentation showing the existence of a business entity.
- Verify the identity of miscellaneous receivable customer if they request information.

Preventing and Mitigating Identity Theft

- Social security numbers are never requested, used, or stored, in the miscellaneous receivable customer information system

- Requests for confidential miscellaneous receivable customer information files are provided only to city staff that are working with the miscellaneous receivable customer information as required for their department

- Customers' bank account information which is stored in the miscellaneous receivable system is maintained in a secure manner. This information is not disclosed to parties outside the miscellaneous receivable system staff.

- Inactive miscellaneous receivable customer files are stored in a locked area.

- All miscellaneous receivable customer system records are password protected.

- The appearance of altered or forged documents prompts further investigation.

- Computer screen darkens or fades out when miscellaneous receivable staff is away from their desk.

- The Accounting Assistant for miscellaneous receivables is designated as the only person who can grant access to the miscellaneous receivable system

APPENDIX B

Parks and Recreation Records Internal Identity Theft Policy
Effective October 20, 2008

PURPOSE: Establish guidelines consistent with the City of Columbia's Identity Theft Prevention Program.

POLICY: Any person or agency requesting information regarding customer's personal information must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

- All credit card and ACH banking information stored in RecTrac database is encrypted throughout the database and cannot be obtained by any user or staff.
- WebTrac (online registration) user name and passwords are set by customer. If customer forgets this information, they must know their security features they set up in order to access such information.
- E-mail and phone requests requesting customer's PIN # for online registration must confirm their mailing address, phone number and security features.
- Faxed requests are not acceptable.
- Refunds and payments are only allowed by the actual customer. There shall be no refunds or transfers of programs by individuals outside the customer's household.
- Governmental agencies; police or prosecutors requesting information must properly identify themselves. These requests should be handled by the Manager or Supervisor.
- Any discussion of the details of customer's personal information outside of the office is never acceptable for any reason.
- Scholarship assistance information shall be stored in a lockable file cabinet. Access to scholarship information shall be limited to those employees requiring access.
- The Department shall maintain an up-to-date list of those employees that are required to have access to personal records.
- Any photocopies made by Manager or Supervisor must have sensitive information (social security number, driver license number) blacked out.

APPENDIX C

Information Systems Internal Identity Theft Policy
Effective April 3, 2008

Relevant excerpts from the
City of Columbia Comprehensive Security Policy
(entire policy may be found online at
http://www.columbia.mo.gov/is/documents/security-policies.pdf)

1.3 Identification and Authentication

1.3.1 Passwords

Passwords confirm that a person is who they claim to be. As such, passwords are extremely important to the security of the City of Columbia Information System. In general, city password policy encourages a balance between complexity, rotation, and user needs. Both lenient and strict policies are generally counter productive to security. This policy instead strives to set standards that, when used together, strike an appropriate balance.

1.3.1.1 Complexity

Passwords should be greater than 8 characters, mix upper and lower case characters, and use symbols. Alternatively, passphrases can be used in the absence of passwords. For example, "AskNotForWhomTheBellTolls" is a very long password and is therefore more difficult to break. Passwords should not be easily guessed. Phone numbers, names of friends, relatives, and pets, and other personal information are generally very easy to guess.

PCI DSS 8.5.10

1.3.1.2 Rotation

Passwords should not resemble previous passwords. For example, "Password12" should not be used if "Password11" has been used before. Where possible, systems and

applications should be set to "remember" old passwords and disallow use of passwords that match or are similar to a previous password. Where possible, systems should be set to store the last 10 passwords.

PCI DSS 8.5.12

1.3.1.3 Password Responsibilities of Users

Users are responsible for choosing passwords that are reasonably complex as defined in 1.3.1.1. Users must be able to use their passwords day to day and are therefore responsible for choosing passwords that will be meaningful enough for them to remember. Users are allowed to write down their password if they are unable to remember it. If a user chooses to write down his/her password, he/she must follow these rules:

a) Their user id must not accompany the password

b) The written password must be stored in a locked location to which ONLY the user has access. The written password must never be hidden in an unlocked location.

c) The password should not be disposed of until it is no longer valid. If possible, the user should shred the password.

Users must recognize the importance of password privacy. Users must never share their password with anyone. Users must never ask each other for their passwords. Departments must make sure that business operations are such that users never need to share credentials. IT staff must never ask users for their passwords and users must understand that IT staff will never do so.

1.3.1.4 Creating and resetting passwords

Temporary passwords, whether created due to account creation or password reset, are subject to section 1.3.1.1. A temporary password created for one user should not be the same as a temporary password created for another user. Instead, temporary passwords should be random and unique.

Users should call the Helpdesk to have passwords reset for every system and application. The Helpdesk should generate a temporary password, set the password to expired, and give the user the new password. The Helpdesk should encourage the user to immediately change the password. When passwords are reset the password should never be available to the user in an electronic form. The Helpdesk shall reset the password then give the new password to the user over the phone.

When a user requests a password reset, a work order shall be immediately created before continuing. The technician resetting the passwords shall check the SecTrack application to ensure the user is allowed to use the system for which he/she is requesting the password change. If the user is not authorized to use the system for which he/she is requesting access, the technician shall inform the user that he/she needs access through the SecTrack system and he/she should speak to his/her supervisor. The success or failure of the password reset will be documented in the work order. The temporary password should not be put in the content of the work order.

Users should never be allowed to reset their password without sufficiently proving that they are who they claim to be. Systems and applications that have "Forgot Password" links should direct users to the Helpdesk instead of providing a password reset method. Helpdesk employees must take responsibility for ensuring that the person requesting a password change is who they claim to be.

If the helpdesk employee cannot verify the user's identity, the Helpdesk employee may require the user to provide "cognitive passwords," or answers to questions that only the user is likely to know. A list of questions and their corresponding answers will be maintained by the IT department, and when a user calls with a password reset request, three questions will be chosen at random. The user must be able to answer the cognitive password questions before the password is reset.

PCI DSS 8.5.2, PCI DSS 8.5.3

1.3.1.5 Password expire

Passwords shall expire every 90 days. Once a password is expired, the user shall be required to change it. All systems and applications that support password expiration should enforce this policy.

PCI DSS 8.5.9

1.3.1.6 Password Transmission and Storage

Passwords should be encrypted using hash algorithms whenever stored or transmitted. The password hash algorithm used should be evaluated in accordance with the cryptography policy.

PCI DSS 8.4

1.4.3 User privilege audits

Each system and application should have a user privilege audit at least annually. The audit should consist of two parts:

1) Department confirmation that the requested access on file in SecTrack matches the access the department wishes the user to have.

2) The access given matches the access requested in SecTrack.

Satisfies NERC CIP-003-1 R5.2

1.4.4 Account audits

Each system and application should have an account audit at least annually. The audit may be done in concert with the user privilege audit in 1.4.3. The audit should consist of two parts:

1) Enumeration of all user accounts.

2) Determination that each user account has a valid SecTrack request and that the user is still employed by the city.

NERC CIP-003-1 R5.2

1.5 Accountability and risk mitigation measures

1.5.1 Accountability

Every system and application has an accountability mechanism that differs in some way from the mechanisms of other systems and applications. Each system and applications should be evaluated and accountability mechanisms should be enabled and configured according to risk. The following are general guidelines to implementing accountability across multiple independent systems and applications.

1.5.2 Authentication logging

Systems and applications should, where possible, create log entries for authentication attempts, both successful and failed. Log entries should include user identification, date/time stamp, and the device (machine name and/or IP address) from which the attempt originated.

1.5.3 Review of authentication events

Every system and application should have its logs reviewed regularly for possible security breaches. The frequency and content of the log audits may be different for each system and should be risk based.

1.5.4 Last login information

On systems and applications where capability exists, the user should be presented with details about their last successful login. Details should include time, date, place and any other pertinent information specific to the system or application.

1.6 Administration

1.6.1 Clipping level

Accounts should not allow an infinite number of "tries" until the correct password is used. Instead systems and applications should implement a "clipping level" that locks out accounts once a certain number of failed attempts has occurred for a user id. Systems and applications that have an enforcement mechanism for this policy shall have this value set to no more than 6. If possible, the user should not be aware that their account is disabled, only that their login attempt failed. Systems and applications should lock accounts for no less than 30 minutes.

PCI DSS 8.5.13, PCI DSS 8.5.14

APPENDIX D

Columbia Police Department Notification Procedures
Effective October 24, 2008

City of Columbia Employees will routinely be exposed to situations where Identity theft is a concern. It is imperative that staff follow notification procedures to ensure that the interests of both the City of Columbia and potential victims are protected.

Employees will consistently be discussing account and customer information over the phone or in person. It is imperative that the customer identity be established prior to any account services being provided. Employees, at times, will be given conflicting or false customer information. If the information can not be clarified or substantiated by staff to a reasonable degree, the customer will be required to respond in person and show a valid form of photo I.D. Once employees are reasonably satisfied there are no identity theft concerns, services can be provided.

Employees who continue to suspect the customer of identity theft can request the assistance of the Columbia Police Department. Employees should obtain a detailed description of the suspect and be able to provide a short synopsis of the incident. Officers will respond to investigate, determine if a crime occurred and take appropriate action.

Staff will potentially discover instances of identity theft or will be notified by a customer of the crime. Employees will assist victims of identity theft with necessary information and also assist with the investigation. Employees will provide an "Identity Theft Victim Information" sheet to all potential victims. Any victims who suffer a monetary loss and are seeking potential reimbursement from the city of Columbia will be required to file a police report and assist with prosecution.

Employees will call the Columbia Police Department and an officer will respond to investigate. Staff should be prepared to provide the officer copies of original documents or any other pertinent information that can be used for the investigation. If the City of Columbia suffers a loss from the identity theft incident the officer needs to note this in the police report for potential restitution.

Employees discovering incidents of internal theft should obtain enough information for a preliminary police report. Staff should be prepared to work with investigators and gather the following information:

Case preparation guideline for embezzlement or internal theft cases

Major Crimes Division, Columbia Police Department

No one is more familiar with your bookkeeping methods than you or your accountant. Therefore, it is important that you convey that information in a manner that is easy to understand and follow. In order to assist in the investigation and prosecution of your case, it is requested that you provide documentation in the following format.

Document preparation:

When preparing your documentation, place all of the pertinent information into a three-ringed binder that is designed to hold your information secure. Original documents should be used when compiling your initial folder. Once your original binder has been completed, make three copies. Please retain one copy for your records. The original and **two** copies should be submitted to the police. Once your case has been completed, the original documents will be returned to you. **Please remember that a neat and professional product is very important.**

Overview sheet:

The overview is a "brief" narrative that provides enough details of the case that the reader can obtain a clear understanding of the incident. The following information must be included, but is not limited to:

A. Who discovered the theft and how it was uncovered.
B. Who the suspect is.
C. The dates of when the theft started and ended.
D. The theft amount.
E. How the theft was performed.
F. The names of anyone the suspect made statements to about the theft and what was said.

Narrative sheet:

Please provide a "detailed" explanation of the theft. Please include the same information from the Overview Sheet section, plus an explanation of the supporting evidence, i.e. documents, ledgers, receipts, etc. Note: This section should read like a novel, covering every aspect of the case from beginning to end. Your information may be returned for revision, if this section is not thorough. It is vital that you explain all the supporting documents in this section, so it is clear and easy to understand. All documents must be numbered. Numbering each document makes it easier for the reader to locate information, when you refer to specific figures and page numbers. You may also consider using a highlighter to aid in quick location of figures.

Itemized list

This section is composed of an itemized list of each loss, date of the loss and the supporting document page number. A total loss dollar amount should be included at the bottom of this list.

Supporting Documents:

Include all documents relating to this case, which were explained in the "Narrative" section. **If you have any questions; do not hesitate to call the detective handling your case. The investigative office can be reached at (573) 874-7423.**

Finally, employees discovering incidents of computer related crimes (hacking or similar offenses) or where customer information or employee identity theft is at risk should immediately call the Columbia Police Department to file a report and initiate an investigation. (**Emergency 911**; **Non-Emergency 442-6131)**

The following Identity Theft Victim Information is what responding police officers provide Identity Theft Victims:

Identity Theft Victim Information

The City of Columbia requires a Police report and cooperation in the prosecution of the person or persons responsible before any reimbursement of losses will be discussed/determined.

Place a fraud alert on your credit reports and review your credit reports:

Equifax 1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241

Experian 1-888-EXPERIAN (397-3742)
P.O. Box 9532
Allen, TX 75013

TransUnion 1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

When you report to one of these bureaus, they will report to the other two for you, and send you free reports. When you receive your reports, review them carefully. If there are any errors, report that to the credit bureaus by phone and in writing.

Close any accounts that have been tampered with or opened fraudulently, such as credit cards, bank accounts, phone and cell phone accounts, utility accounts, and internet service providers. Either use an Identity Theft Affidavit or ask the company to send you fraud dispute forms if they prefer, if there are fraudulent charges or debits.

The ID Theft Affidavit is to make sure you do not become responsible for debts incurred by the ID thief, so you must provide proof you did not create the debt. You can use the affidavit where a NEW account was opened in your name. Use it ASAP. For EXISTING accounts, your credit company will provide you with their own Dispute forms. The ID Theft Affidavit can be found at www.consumer.gov/idtheft.

If your ATM card is lost, stolen, or otherwise compromised, cancel it. Get a new card and PIN.

If your checks were stolen or misused, close that account and open a new one. Contact the three major check verification companies, and ask that retailers who use their databases not accept your checks.

TeleCheck 1-800-710-9898 or 927-0188

Certegy, Inc.	1-800-437-5120
International Check Services	1-800-631-9656

Call SCAN at 1-800-262-7771 to see if bad checks are being passed in your name.

- **File a complaint with the FTC.**

  FTC Toll-free 1-877-IDTHEFT (438-4338), www.consumer.gov/idtheft TDD 202-326-2502

  Identity Theft Clearinghouse
  Federal Trade Commission
  600 Pennsylvania Ave., NW
  Washington, DC 20580

  - Document everything: Keep originals of all correspondence and documents; send copies as necessary
  - Keep a record of everyone you talk to (names, dates, etc.)
  - Keep all your files FOREVER! If something happens at a later date, you will be glad you did
  - If you believe someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where it was filed. A list is available on the UST website at www.usdoj.gov/ust/
  - If wrongful criminal violations are attributed to your name, contact that law enforcement agency
  - Contact the Department of Motor Vehicles at www.dor.mo.gov/ and ask that your files be flagged
  - If theft of mail was involved, contact the U.S. Postal Inspection Service at www.usps.gov/websites/depart/inspect
  - If phone fraud was involved, contact the Public Utility Commission. If cell phone or long distance service was involved, contact the FCC at www.fcc.gov
  - If your social security number was involved, contact the Social Security Administration at www.socialsecurity.gov
  - If tax fraud was involved, contact the IRS at www.treas.gov/irs/ci
  - **You can find much more information about Identity Theft, with more help and guidance, at the FTC's website at www.consumer.gov/idtheft**
  - ***Information provided comes directly from the FTC's website at www.consumer.gov/idtheft***

Appendix E

Identity Theft Training Program
Effective December 1, 2008

Training Protocol

I. Introduction

a. What is Identity Theft?

II. Red Flag Legislation

a. The Federal Trade Commission's Red Flag Rule (Implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003, pursuant to 16 C.F.R. 681.2.
b. Complying with the Red Flag Rule
c. How flexible is the Red Flag Rule?

III. The City's Identity Theft Prevention Program

a. Departments who must comply
b. Examples of Red Flags
c. What is your role and responsibility?

IV. Identity Theft

a. What is Identity Theft?
b. How does it happen?
c. How do you protect yourself from it?
d. What do you do if you're a victim?

V. How to Report

a. Your expectations
b. Notifying Law Enforcement
c. Your Assistance if investigation involved
d. What to do if a Law Enforcement response is not necessary

VI. Resources

Appendix F

Needs Assessment
Effective December 1, 2008

Conducting a Needs Assessment

Opening a New Record

Identify the steps in establishing a new record for a customer.

1) What identification is required? How do you obtain identifying information and verify identity? _____

2) Do they need to make the application in person or can they send in the information in an alternate form? Telephone or other? _____

3) Does the Department use consumer reports in the application process? How? Establish deposit? Approve or deny services? _____

4) Does the Department have policies and procedures that define red flags for identity theft and actions for mitigation? _____

5) What happens to the hand written notes made by the Department Representative in the application process? _____

6) Is the computer screen visible to others during the application process? _____

7) Who has access to data once entered? Does the Department Representative lock computer when not at desk? _____

8) If applicant gives address, bank account, date of birth or social security number verbally to Department Representative, what precautions are taken from others hearing? _____

9) Once personal identification information is entered by Department Representative, where and how can it later be retrieved? _____

10) What safeguards are currently built into the application process? _____

11) What safeguards would you like to implement? _____

12) Which employees have access to information – is it on a "need to know" basis? _____

13) Is any customer personal information carried into the field on a laptop? _____

Map out the steps that occur when opening a new account. Is customer identification validated? Is so, how? Trace the flow of secured information.

Customer Initial Contact

Service is established

Needs Assessment continued

Monitoring an Existing Record

Identify the possible red flags that may exist in the following procedures:

- ✓ Authenticating transactions for existing customers
- ✓ Monitoring activity/transaction of customers
- ✓ Verifying the validity of change of billing address
- ✓ Does the Department have policies and procedures that define red flags for identity theft and action for mitigation for existing records?

Does your Department use passwords or some form of security access?

_____
_____
_____
_____

Describe your process for verifying validating the following:

Check by phone_____

Credit Card Number_____

Are receipts ever printed? If so, what part of number is exposed?_____

In what manner have customers attempted to fraudulently represent themselves as someone else in a transaction in an existing account?

_____

What safeguards are currently built into monitoring existing record(s)?

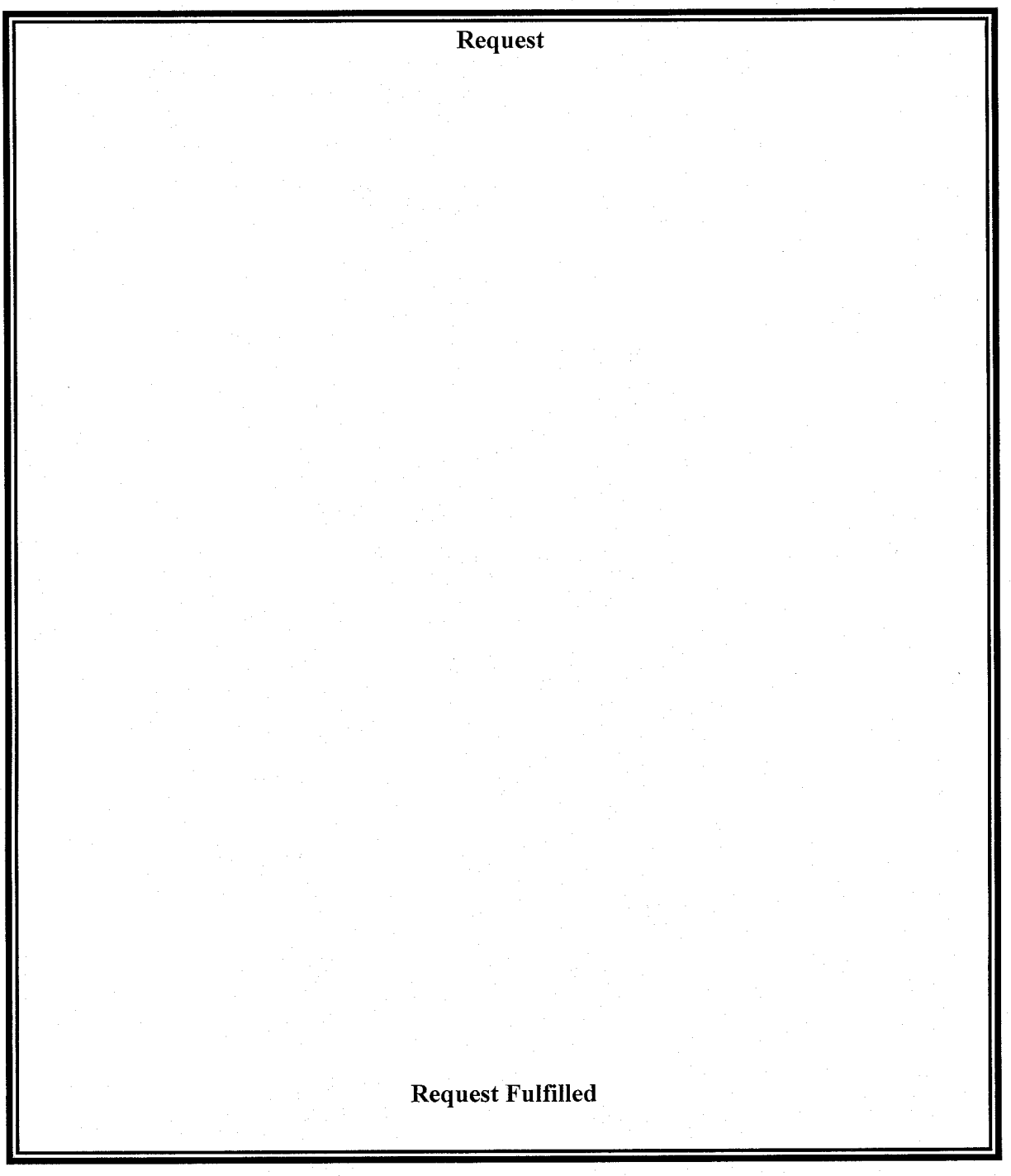
_____
_____
_____
_____

What safeguards would you like to implement?

_____
_____
_____
_____

Map out the ways customers, 3rd parties and others access existing Records.

How do you authenticate transactions for existing Records?



After you have mapped out the flow of information, identify possible areas where the protection of secured information could be improved.

SUMMATION360™

TASK MATRIX for COLUMBIA - PHASE 1: IVR, Web-Pay Now, Web-"My Account" Portal, Customer Notifications, TWI PPS

Task #	Event	Task Description(s)	Completion Criteria
Stage 1: Pre-Implementation			
1.1	Signed Contract	Provide notice to proceed.	TWI receives billable documentation (Purchase Order or Contract); Columbia is contacted to schedule kick-off call
1.2	Project Kick-off Call	1) Project Team Introductions 2) Review Scope of Work 3) Review Pre-Implementation Questionnaire Including Columbia Deliverables	Kick-off call follow-up email sent; Columbia provides timeline estimates to complete its assigned deliverables
1.3	Application Programming Interface (API)	The necessary API(s) required to support the Summation360 features are obtained/created and installed. (NOTE: Columbia will wrap all required stored procedures (existing or new) into a web service. The features contained within the initial release of Summation360 will be a function of the data provided by the existing API framed within the fixed Summation360 product interfaces.)	API access is provided to TWI including all necessary information to establish connectivity to both production and test environments.
1.4	Secure Test Environment	Provide secure client-based IPsec tunnel VPN (if applicable) or establish communication to the API through Columbia's firewall for hosted deployments.	TWI is able to access and communicate to the relevant areas of Columbia's environment
1.5	Payment Solution Requirements Completed	TWI will work with Columbia to complete the on boarding process for the City to use TWI Payment Processing Services (TWI PPS). All of the necessary documentation is completed and signed off on.	TWI establishes the payment gateway. Check processing method clearly defined; details surrounding fees or advanced payment features (e.g. Recurring) including release schedule, are outlined
1.6	Electronic Bill Presentment & Paperless Billing Processes	Processes and action items related to the implementation of electronic billing features identified during presale discovery are reviewed. Features include email bill reminders, paperless billing, and electronic bill presentment.	All action items required to support electronic billing processes are completed; strategy regarding the release of these advanced project features are outlined. (NOTE: eBill/Paperless features currently scheduled for Phase 2.)
1.7	Complete Pre-Implementation Packet	Columbia works to complete all tasks assigned within the pre-implementation packet, which include business rules defined by the members of the department involved in the application configuration.	Completion of pre-Implementation deliverables
1.8	Data Validation Session	During a conference call, TWI will run test data through the API and confirm the values with Agency staff to confirm the accuracy of the data so the correct business rules can be applied. TWI estimates release to Columbia of Phase 1 features at 6-8 weeks from the successful completion of Data Validation.	Project release target dates set. Additionally, Columbia/TWI project management resources will target planned timelines for subsequestion phases
Stage 2: Implementation			
2.1	Application Configuration	Configuration of the application proceeds, which includes information collected in the pre-implementation packet. Routine updates on progress are provided identifying any issues that may affect target dates.	Pre-Implementation items configured into application
2.2	Finalize Application Configuration	Application Configuration is finalized and installed in the production environment.	Remote diagnostic tests successfully completed
Stage 3: Phase 1 Release			
3.1	Phase 1 Release	Phase 1 features/functionality released to Columbia for verification and testing. Columbia is provided with testing information, including guidelines on reporting any issues.	Project release document delivered (can be relative to specific released features)
3.2	Production Testing	As any configuration issues are resolved, testing of the production API connectivity and live payments is coordinated. Upon successful completion of the last testing milestones, the project is considered complete.	Project completion notice is sent (can be relative to specific released features); TWI continues to support Columbia's efforts to move the application into production. Phase 2 Impementation begins, the completion of which is follwed by Phase 3.

Summary Description of Stage 1 - Pre-implementation: TWI issues an internal notification to proceed upon receipt of signed contract from Columbia. Craig Ferguson, Director of Engineering and TWI Project Manager, contacts Columbia's designated Project Manager and, working with Columbia's schedule, arranges the Project Kick-Off Call. TWI will provide Columbia with a pre-implementation questionnaire that outlines all of the action items and deliverables that must be completed prior to Configuration. Once TWI has received all customer deliverables and a successful Data Validation Session is conducted, the project moves into the Implementation stage. The duration of the Pre-Implementation Stage will be based primarily on the completion of Columbia's action items as described in the Stage 1 - Pre-implementation above.

Summary Description of Stage 2 - Implementation: TWI staff begins configuring the application. Actual implemention timelines can vary depending upon specific project issues but become clearer as progress is made. TWI will provide to Columbia apdates to the preliminary timeline if any risks or improvements become evident. Upon completion of application configuration, TWI conducts its internal quality assurance for the deliverables and releases the application for review and testing by Agency staff. Based on TWI's experience with Columbia, the understanding of the existing API, the availability of project resources, and other factors, TWI estimates the duration of the Implementation stage at 6-8 weeks.

Summary Description of Stage 3 - Project Release: After the project is released to Columbia for review, Craig will continue to work with Columbia until any configuration issues with the product are resolved. Once the issues are addressed, Craig will coordinate the completion of final testing milestones which include testing against the production database and live payment testing. Completing the initial project review and production testing milestones typically takes 1-2 weeks and marks the completion of that phase of the project

Subsequent Project Phases: TWI currently plans for Phase 2 of the Columbia project to be the Implementation/Release of Web - Paperless/eBilling and Phase 3 to be the Implementation/Release of Web - Mobile. As indicated above, Columbia/TWI Project Management will determine targeted timelines and release schedules during Stage 1.8 of Phase 1.

Requirement	Supported Yes/No	Please explain:
Customer Accounts		
Account status displayed (delinquent, active,)	yes	
When payment is made on a delinquent account staff will be automatically contacted	yes	
Provides method of recovering lost passwords online	yes	
Does the system provide the customer all the associated accounts for their customer ID and allow them to click on the accounts to add without having to key each one in.	**no**	**Customers will need to link accounts manually (this is mainly for security purposes)**
Includes up to 13 months of consumption, bill and payment history with data view and bar graphs	yes	
Payment Processing		
Ability to add a menu link to an internal bank transfer auto pay sign up form and other forms and related services.	No, not as the product sits now but can be added.	Once they get to the payment screens they would not be able to link directly to an ancillary payment process, they would first need to go back to Columbia's home page. Should the city desire this functionality, TWI can add this after implementation.
Accepted credit cards can be defined by the City at any time without change fees	yes	
Updates financial system to show pending payments once a payment has been submitted; customers will see that their payment is being processed or has been applied	yes	
Provides customer validation of payment information, to include clearly identifying the convenience fee, prior to submission and ability for customer to cancel or edit payment.	yes	
Provides a printable payment receipt	yes	
Description on customers credit card/bank statement will make it clear that it is a payment to the City of Columbia for utility payments.	**yes**	
Emails customers the details of their payment	yes	
Billing		
Uses our existing pdf version of the utility bill	yes	
Will flag customers when they have viewed their bill online during the current payment period	No	We are tracking bill reminders but we are not currently tracking the fact that they have opened their bill.
Security		
Uses 128 bit encryption to secure transactions	yes	
Allows secure storage of **multiple** credit card and banking profiles for a customer	yes	
PCI compliant	**yes**	
Uses customers credit card number, expiration date and CVC code to validate authenticity	yes	
Miscellaneous		
Look and feel of the utility billing system can be edited by City staff.	No	Generally the look and feel are set as part of

		the product. There is some flexibility on colors and logos are incorporated along with banners… should they change at the at city, TWI would make the necessary changes.
Allows staff to post messages on initial log in landing page, and each page of the payment process.	Yes	
Provides accounting report where staff can review transactions, payment status, and all relevant information. **Reporting feature should allow the search for a specific payment in the system by any relevant data fields. An error code look up feature is highly desired.**	**Yes**	
Log to track account access, payments and bills views by account number.	**Yes**	
Provides statistics reports for page views, sessions, online transactions, telephone transactions, and e-bill users broken down by month or year.	Yes	
Application is Section 508 ADA compliant	Yes	
When text messaging is used there will be an alert or other means for staff to know that the 160 character limit has been reached	.Yes	
To avoid unintended selection, the system will make it clear when high volume call out has been selected.	Yes	

Source: Finance

Agenda Item No:

To: City Council
From: City Manager and Staff

Council Meeting Date: October 1, 2012

Re: Contract with Tele-Works Incorporated ("TWI") for utility payment solution and charging a convenience fee.

EXECUTIVE SUMMARY:

A resolution authorizing the City Manager to enter into a Contract with Tele-Works Incorporated ("TWI") for the implementation of the Summation 360 Solution Suite, a hosted, multi-channel billing, payment, and automation solution for utility billing and incorporation of a convenience fee.

DISCUSSION:

At Council's request, the Department of Finance has worked with the current on-line and telephone billing payment provider to upgrade the online application and incorporate a convenience fee for all payments made via the internet or telephone. The implementation of this solution will reduce the City's cost by approximately $350K - $400K. A convenience fee of $4.60 per $1,000.00 payment will be charged to the customer for payments made by credit card or e-check via the internet or telephone.

FISCAL IMPACT:

Approx. $350K - $400K savings in credit card fees and software maintenance cost.

VISION IMPACT:

http://www.gocolumbiamo.com/Council/Meetings/visionimpact.php

SUGGESTED COUNCIL ACTIONS:

Approval of the resolution authorizing the City Manager to enter into the contract with Tele-Works Incorporated .

FISCAL and VISION NOTES:					
City Fiscal Impact Enter all that apply		**Program Impact**		**Mandates**	
City's current net FY cost	$450,000.00	New Program/ Agency?		Federal or State mandated?	No
Amount of funds already appropriated	$0.00	Duplicates/Epands an existing program?	Yes	**Vision Implementation impact**	
Amount of budget amendment needed	$0.00	Fiscal Impact on any local political subdivision?	No	Enter all that apply: Refer to Web site	
Estimated 2 year net costs:		**Resources Required**		Vision Impact?	
One Time	$0.00	Requires add'l FTE Personnel?		Primary Vision, Strategy and/or Goal Item #	
Operating/ Ongoing	$0.00	Requires add'l facilities?		Secondary Vision, Strategy and/or Goal Item #	
		Requires add'l capital equipment?		Fiscal year implementation Task #	